Registratiekamer

Information and Privacy Commissioner/Ontario

CONTENTS

Privacy-enhancing technologies:

The path to anonymity
Revised Edition

Achtergrondstudies en Verkenningen 11

Editors: Ronald Hes and John Borking

PRIVACY-ENHANCING TECHNOLOGIES:

The path to anonymity
Revised Edition

Achtergrondstudies en Verkenningen 11

Registratiekamer, The Hague, August 2000

ISBN 90 74087 12 4

Reports in the serie *Achtergrondstudies en Verkenningen* (Background Studies and Investigations) are the result of enquiries carried out by or on behalf of the *Registratiekamer*. The Registratiekamer hopes that the publication of these reports will stimulate discussion and shape public opinion on social developments which have an impact on the personal privacy of the citizenry.

Privacy-enhancing Technologies: the path to anonymity
The Hague, 2000

Revised edition of:
Rossum, H. van, e.a. (1995). *Privacy-enhancing Technologies: the path to anonymity*.
Den Haag: Registratiekamer. ISBN 90 346 32 024

ISBN 90 74087 12 4

Druk: Sdu Grafisch Bedrijf bv

Table of contents

Part 1 Summary

At the present time, an individual is required to reveal his identity when engaging in a wide range of activities. Every time he uses a credit card, makes a telephone call, pays his taxes, subscribes to a magazine, or buys something at the grocery store using a credit or debit card, an identifiable record of each transaction is created and recorded in a computer database somewhere. In order to obtain a service or make a purchase (using something other than cash), organizations require that you identify yourself. This practice is so strong that it is simply treated as a given, an individual's identity must be collected and recorded in association with services rendered or purchases made. But must this always be the case? Are there no situations where transactions may be conducted anonymously, yet securely? We believe that there are, and will outline a number of methods and technologies by which anonymous yet authentic transactions may be conducted.

1 Background

Consumer polls have repeatedly shown that individuals value their privacy and are concerned about the fact that so much personal information is routinely stored in computer databases over which they have no control. Protecting one's identity goes hand in hand with the option to remain *anonymous*, a key component of privacy. While advances in information and communications technology have fueled the ability of organizations to store massive amounts of personal data, this has increasingly jeopardized the privacy of those whose information is being collected. Minimizing the amount of identifying data would restore privacy considerably, but would still permit the collection of needed information.

When assessing the need for identifiable data during the course of a transaction, the first key question is: how much personal information/data is truly required for the proper functioning of the information system involving this transaction? This question must be asked at the outset prior to the design and development of any new system. But this is generally not the rule today. This question is rarely asked at all, since there is such a clear preference in favour of collecting identifiable data: 'the more the better'. However, with the growth of networked communications and the ability to link a wide number of diverse databases electronically, people will become more and more reluctant to leave behind a trail of identifiable data. What is needed is a paradigm shift away from a *more-is-better* mindset, to a minimalist one. Is it possible to minimize the amount of identifiable data presently collected and stored in information systems, but still meet the needs of those collecting the information? We believe that it is.

The technology needed to achieve this goal exists today. We describe some of the privacy-enhancing technologies that permit one to engage in transactions without revealing one's identity by introducing the concept of an *identity protector*. The notion of *pseudonimity* will also be introduced as an integral part of protecting one's identity. These technologies are available now and within our reach; what is needed is the *will* to implement *privacy-enhancing* technologies instead of the *tracking* technologies that are in use today.

When organizations are asked what measures they have in place to protect privacy, they usually point to their efforts at keeping information secure. While the use of security measures to prevent unauthorized access to personal data is an important component of privacy, it does not equal privacy protection. The latter is a much broader concept which starts with the questioning of the initial collection of the information to ensure there is a good reason for doing so and that its uses will be restricted to legitimate ones of which the data subject has been advised . Once the data has been collected, security and confidentiality become paramount. Effective security and confidentiality will depend on the implementation of measures to create a secure environment

Alternatively, instead of restricting the focus to security alone, a more comprehensive approach would be to seek out ways in which technology may be used to enhance the protection of informational privacy or data protection. We use the term *privacy-enhancing* to refer to a variety of technologies that safeguard personal privacy by minimizing or eliminating the collection of identifiable data.

Not only are measures that safeguard privacy becoming an important mark of quality, but increasingly, critical consumers demand that organizations pay attention to their privacy concerns. Social acceptance of gathering personal information, without adequate assurances of protection, appears to be declining. Not only do consumers wish to maintain control over their personal data and be informed of its uses, insufficient protection is also a motive for consumers to take their business elsewhere to companies that follow privacy-protecting practices.

2 Privacy laws and codes of conduct

Respect for individuals' privacy, particularly with respect to the computer processing of personal data concerning oneself, is a fundamental principle underlying data protection. In Europe, *data protection principles* may be found in several instruments such as:

- the Council of Europe's Convention 108 (Treaty for the protection of persons with regard to automated processing of personal data, Council of Europe, 28 January 1981 (1988 Official Journal of Treaties, 7))
- the Data Protection directive 95/46 of the European Parliament and the Council of 24 October 1995 concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data.

These principles have the goal to ensure that personal privacy is safeguarded when new information technology applications are developed. The principles are reflected in various European laws and regulations, such as the Data Protection directive 95/46 and the Dutch Data Protection Act (Wet persoonsregistraties, to be succeeded by the Wet bescherming persoonsgegevens). In addition, the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (September 1980) are internationally acclaimed as a *code* of *fair information practices* with respect to the treatment of personal information.

One of the basic principles in the OECD guidelines, Convention 108 and Directive 95/46, is the principle of *purpose specification*. The quantity and nature of personal data that an organization is permitted to collect should be limited by the purpose of the collection. The primary rule is that the data be relevant and sufficient, but not excessive, for the stated purpose. In other words, the personal information to be collected must be necessary to carry out the stated purpose.

This principle also seeks to ensure that restraint is exercised when personal data are collected. In accordance with this principle, one may question when identifying data is being sought from individuals where it is not necessary to do so. This is associated with the *use limitation principle*, where the purpose specified to the data subject at the time of the collection restricts the use of the information collected. Thus, the information collected may only be used for the specified purpose (unless consent has been obtained for additional uses).

Another important data protection principle is *transparency or openness*. People have the right to know what data about them has been collected, who has access to that data, and what the data is being used for. The principle of transparency simply means that people must be made aware of the conditions under which their information is being kept and used.

The principle of transparency also sheds light on the logic behind the processing of collected data. The demand for information in a situation that does not strictly require it must be questioned. Indeed, the collection and use of personal data for identification purposes when not truly necessary (where alternatives are available), cannot be justified on the basis of the principles noted above. Since these data protection principles are incorporated into most privacy laws such as the Dutch Privacy Act, or the EU-directive 95/46, the unnecessary collection of identifiable data may have a direct bearing on compliance with these statutes.

3 Information systems

An information system is a system that provides organizations with the information required to conduct various activities. There are generally three types of information systems: transaction-processing systems, programmed decision-making systems, and decision-support systems. Transaction-processing systems collect and keep track of information relating to a transaction. Examples range from direct marketing systems, mail order catalogue purchasing systems, telephone records systems, and so forth.

Programmed decision-making systems process data in accordance with formal, structured procedures. The system is programmed, on its own, to handle the entire order from the time it is received to completion, without any human intervention. Examples include hotel reservation systems, payroll accounting systems, money transaction systems for automatic teller machines, flight reservation systems, etc.

Decision-support systems assist in the decision-making process by using the information collected to either generate potential solutions or additional information to assist in the decision-making process. Examples include systems for calculating mortgages, management information systems, recommended itinerary systems, etc.

The one common feature of all of these systems is that their use entails the collection and processing of personal information. Whenever an individual (the user) comes into contact with an information system, the service provider usually requires that he identify himself.

3.1 The structure of an information system

The elements of an information system consist of the following: user representation (containing a means of identification), service provider representation, and a database(s) containing the data required for the information system to function. The database usually consists of two files, the privileges file and the audit file. The privileges file contains the user's privileges (which the service provider would check to see whether he/she was eligible for the various services offered). The audit file records the use of the information system and can charge the user of a service or track what services were used by whom, at what times. Using the example of a health club, the privileges file would contain a record of the user's entitlements, i.e., that a particular user was entitled to use certain services such as the use of the tennis facilities (five times a month), the squash courts (four times a month), but not the golf course (for which the user had not paid the required additional fee). The audit file would keep track of the actual uses of the various privileges and charge the user a per-use fee for any additional services the user was not entitled to (e.g., playing golf).

A user representation can take the form of an account number, a membership card or a smart card. A service provider representation represents the interests of the organization and controls access to the organization's various resources (through passwords, tiered levels of authorization to increasingly sensitive information, etc.)

3.2 The processes in an information system

The use of an information system entails the following processes: authorization, identification and authentication, access control, auditing and accounting. We refer to a process as an exchange of information between two or more elements within the information system. In conventional systems, the user's identity is usually viewed as being essential to the performance of all the above processes. For example, identity is used within the authorization process to identify and record instances involving a user's privileges. Once the user's identity has been collected, it will travel through the various processes involved in the information system. We will suggest that this need not be the case. One must examine whether the user's identity is truly required for the operation of each of these processes.

We claim that a user's identity is only necessary during the processes of authorization and accounting. For the processes of identification and authentication, access control, and audit, a user's identity may be sheltered through some type of *identity protector*. We will describe how technologies of privacy may be used to separate a user's true identity from the details of the user's transactions through the use of *pseudo-identities*.

4 The identity protector

An identity protector may be viewed as an element of the system that controls the release of an individual's true identity to various processes within the information system. Its effect is to cordon off certain areas of the system which do not require access to true identity. The identity protector works in such a way as to protect the interests of the user. One of its most important functions is to convert a user's actual identity into a pseudo-identity, an alternate (digital) identity that the user may adopt when using the system.

Alternate identities also exist in conventional systems such as bank account numbers, social insurance/social security numbers, health insurance numbers, etc. But these cannot be viewed as pseudo-identities since they may easily be linked to a user's true identity. In privacy-protective systems of the future, the identity protector would most likely take the form of a smart card controlled by the user, which could generate pseudo-identities as desired.

An identity protector performs the following functions:

- generates pseudo-identities as needed;
- converts pseudo-identities into actual identities (as desired);
- combats fraud and misuse of the system.

Since the identity protector is under the control of the user, he/she can set it to perform a variety of functions such as revealing his or her actual identity to certain service providers, but not to others. When an identity protector is integrated into an information system, the user may use the services or engage in transaction anonymously, thereby strongly increasing privacy.

When an identity protector is introduced into an information system, two domains are created: an *identity* domain and a *pseudo* domain, one in which the user's actual identity is known and accessible, and one in which it is not. The identity protector separates the two domains and may be applied anywhere in the system where personal data can be accessed. A simple guideline for designers of new information systems is to minimize the identity domain wherever possible and maximize the pseudo domain.

The identity protector permits the designer of a system to minimize the collection of personal data stored in the database. In effect, the service provider would not record the privileges or activities of the users under their true identities but rather, under their pseudo-identities. While the service provider must be able to determine what a user is authorized to do, this may be accomplished without learning the user's true identity. Since the identity protector acts as an intermediary between the user and the service provider, it must be trusted by both parties. However, there is no disadvantage to service providers since their ability to verify the user's privileges/eligibility for services remains intact. Indeed, the identity protector is designed in such a way so as to prevent fraud and improper use. The latter can take various forms ranging from prevention, detection, and correction. It can prevent the user from using his/her anonymity as a shield to commit fraud, and, in appropriate circumstances, can lead to having the true identity of the user being revealed to the

service provider and/or the authorities. For example, cryptographic techniques may be used to prevent a sum of money (digital cash) from being used anonymously more than once, or a service being used without being charged to the user.

5 Implementation techniques

Thus far we have discussed the theoretical concept of an identity protector in the design of systems that would permit individuals to interact anonymously with service providers. Below, we outline several specific techniques for introducing an identity protector into an information system. Specifically, encryption techniques involving digital signatures, blind signatures, digital pseudonyms and trusted third parties are described. Additional readings are provided in Part 2 of this report.

5.1 Digital signatures

A digital signature is the electronic equivalent of a handwritten signature. Just as a signature or personal "seal" on a document is proof of its authenticity, a digital signature provides the same, if not better, authentication. It provides the necessary assurance that only the individual who created the signature could have done so, and it permits all others to verify its authenticity. A particular type of encryption, *public key encryption*, considered to be an extremely reliable and secure form of encryption, forms the basis for digital signatures.

In a public key system two keys are created for each individual: one private, one public. The private key is known only to the individual while the public key is made widely available. When an individual encrypts a document with his or her private key, this is the equivalent of signing it by hand since the private key is unique to that individual alone. Any third party may decrypt the message using the individual's public key, which corresponds only to his/her private key. If the document is successfully decrypted, then one has the necessary assurance that it could only have been created by that individual. Otherwise, one would not have been able to decode it. Digital signatures thus provide proof of a document's authenticity, that the document originated from the sender. For a more detailed description of this cryptographic technique, please refer to Part 2 of this report.

5.2 Blind signatures

The blind signature, created by David Chaum of Digicash, is an extension of the digital signature, but with one critical feature added: it ensures the anonymity of the sender. While digital signatures are intended to be identifiable and to serve as proof that a particular individual signed a particular document, blind signatures provide the same authentication but do so in a non-identifiable manner. The recipient will be assured of the fact that the transmission is authentic and reliable, but will not know who sent it. One application involving blind signatures is the use of *digital cash* which may be used as an electronic form of payment that can be transmitted over computer networks. Just as cash is anonymous, digital cash is anonymous in that it cannot be traced back to a particular individual, it is considered to be *unconditionally untraceable*. However, the service provider is assured of its authenticity; all that is missing is the ability to link the transaction with a particular person. In describing his system of blind signatures, Chaum adds that it also provides the much needed protections against fraud and abuse of the system.

5.3 Digital pseudonyms

A digital pseudonym is a method of identifying an individual through an alternate digital or pseudo-identity, created for a particular purpose. It permits users to preserve their anonymity by concealing their true identities. While users are not known to service providers in the conventional sense, they are, nonetheless, known by their pseudonyms for the purposes of conducting transactions.

Digital pseudonyms are build upon the blind signature technique. However, in this instance, it is the service provider who assigns privileges to a given pseudonym (user) by creating a blind signature. The user keeps the allotted privileges (for example, five uses of the tennis courts per month), and uses them as desired.

5.4 Trusted third parties

A trusted third party is an independent third party who is trusted by both the user and service provider alike (comparable to a *digital attorney*). This party can be entrusted with keeping such things as the master key linking digital pseudonyms with the true identities of their users. The trusted party knows that the relationship between a user's true identity and his/her pseudo-identity must be kept completely secret. However, if certain conditions require it, the trusted party will be permitted to reveal the user's identity (under previously agreed upon terms) to a service provider. The conditions under which an individuals identity would be revealed must be known to both user and service provider prior to entering into an agreement with the trusted party.

5.5 Moving from conventional technologies to privacy-enhancing technologies

The most important prerequisite for development in the direction of privacy-enhancing technologies is to ask from the outset whether identifiable information is truly needed when a new information system is being conceived, or an existing system upgraded. The creation of some form of identity protector within the system must be a crucial part of the design phase. To recap, the identity protector is a term for all those functions within an information system that protect the user's true identity, such as the creation of pseudo-identities. A pseudo-identity is a pseudonym that the user may assume for the purpose of engaging in a particular transaction or service. The guiding principle should always be to keep the identity domain as small as possible, thereby maintaining the absolute minimum amount of identifiable information. The actual implementation of an identity protector may be done in a number of ways, usually involving advanced encryption techniques.

The point to stress is that it is indeed possible to collect less identifiable data, or unlink the data from an individual's true identity through the use of pseudo-identities. It is only the application of Privacy-Enhancing technologies that is lacking, not the technologies themselves.

2 Privacy-enhancing Technologies: the path to anonymity

1 Introduction

In this part of the report we present a theoretical study conducted by the Registratiekamer in collaboration with the TNO Physics and Electronics Laboratory (TNO-FEL), Telematics and Information Security Group.

1.1 Methodology

This study addresses two central questions:

- What conditions must be kept in mind when engineering an information system in order to guarantee that the system be used effectively and efficiently without revealing the user's identity?
- What types of information and communication technology can contribute towards achieving this goal?

The Registratiekamer outlined the general framework and guidelines of this study. TNO-FEL made an inventory of the information and communication technological (ICT) possibilities to separate the use of the information system from the identity of the user. A few models are presented to serve as examples to designers, developers and marketers when setting up information systems.

1.2 Overview of this report

Chapter 2 defines the concept of information systems. There is a great diversity in information systems, and the system used generally depends on the environment in which it functions. Each information system has certain basic elements and processes in common. These elements and processes can be used to construct a model of an information system, which can then be used to examine whether the various information system processes contain identifying personal data.

Chapter 3 takes a closer look at the privacy-enhancing technology concepts introduced in chapter 2. The information system model is expanded in several places to include identity protectors to safeguard users' privacy. Examples illustrate how these models with integrated identity protectors are used.

Chapter 4 explores a number of potential techniques for the implementation of privacy-enhancing technology in information systems. The end of the chapter introduces a flow diagram for the design of new information systems.

2 Information systems and identity use

The current generation of information systems make use of the user's identity at various points in the system. In this report, a *user* is defined as someone who uses the information system, in whatever capacity. The central question is whether it is necessary for the system to know the user's identity. A model is presented to examine how an information system functions. The model developed serves as a basis for further elaboration of the privacy-enhancing technology concept. It is essential when developing a model to know what the term information system entails. What is the purpose of such *information systems*, how do they work and what are they made of? The next section will address these questions. Subsequently, the difference is explained between the current generation of information systems and information systems based on privacy technology.

2.1 What is an information system?

Information systems serve to provide information required for performing goal-oriented activities (Bemelmans, T. M. A., 1987). Performing can be understood as the planning, conducting and monitoring of specific activities. The scope and nature of information systems display a great degree of diversity, however. They may support a process that only involves a few people, in which case information systems are limited in structure and fairly transparent. On the other hand, there are also information systems utilized by people who do not necessarily belong to the same organization. Nor does the information system have to be limited to one organization. An information system for internal use can also be used for inter-organizational and international data flow.

Information systems can be divided into three types: transaction-processing systems, programmed decision-making systems and decision-support systems (Bemelmans, T. M. A., 1987). *The transaction-processing systems* register a transaction. Examples include:
- entrance registration systems
- mail registration systems
- order registration systems
- telephone records
- pharmacists' systems

*Programmed decision-making system*s process data according to formalized, structured procedures. The system completes the entire order, from the time of its receipt to its completion, often without any human involvement. Examples include:
- hotel booking systems
- wage accounting
- money transaction systems for automatic teller and payment machines
- financial aid systems
- flight reservation systems
- hospital information systems
- ticket systems
- voting machines

As the name suggests, *decision-support systems* assist decision-makers in making decisions. These systems use the information entered to generate potential solutions or other information on the basis of which the decision can be made. Examples include:
- systems for calculating mortgages
- direct marketing systems

– address systems
– recommended itinerary systems
– management information systems

Although information systems have widely diverging purposes, they have one thing in common: their use entails the processing of personal data. Obviously, each information system operates within a certain environment, and thus has a relationship with that environment, such as links with other automated or non-automated information systems as well as the person using the systems and internal and external organizations.

Information systems consist of four components: organization, personnel, procedures and technology. All of these components are crucial to the proper functioning of the systems. This study focuses on the technical set-up of information systems, which determines the degree of protection of the user's privacy. Where necessary, attention will also be paid to the other components.

2.2 Conventional and privacy information systems

The terms *conventional information systems and privacy information systems* are used to denote the information systems mentioned in the preceding section and those which protect user's privacy, respectively. Conventional information systems generally record a high amount of information with a high identification content. This means, of course, that it is easy to link the data to a private individual. Privacy information systems are systems which only reveal the user's identity to combat fraud.

There are two options for privacy information systems. The first is not to generate or record data at all. The second option is to not record data unique to an individual, identifying data. The absence of identifying data renders it impossible to link existing data to a private individual. A combination of the two options offers a third alternative.

By applying the potential forms of privacy-enhancing technology, a conventional information system can be transformed into a privacy information system. The study focuses on the second possibility offered by privacy-enhancing technology: omitting data linked to a person, i.e. identifying data.

2.3 Identity in the information systems

To determine whether a user's identity is, in fact, required for the proper working of an information system, its functions must be evaluated and the following questions answered: Which elements of an information system is identity used for? For which processes? The following sections first define the elements and then the processes of an information system. Each time individual processes are discussed, the following question will be asked: Is the user's identity required for the information system to function properly?

2.3.1 Elements of the information system

A (technical) model of an information system contains four separate elements: user representation, service-provider representation, database, and services (see figure 2.1).

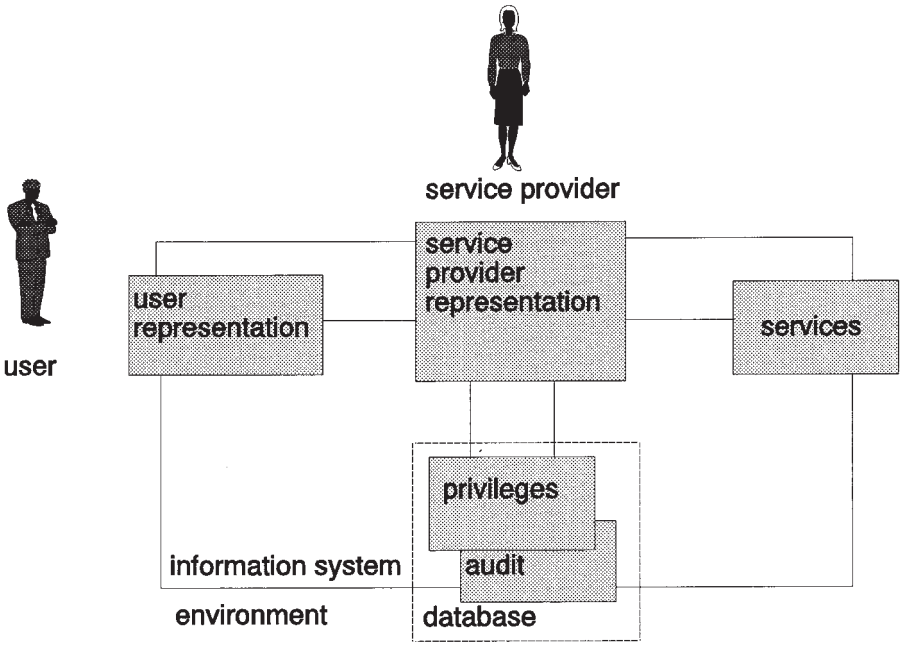

Figure 2.1: A (technical) model of an information system

The *user representation* is the representation of the user - a private individual - within the information system. A user representation will generally be a process that performs certain functions at the user's request, and consists of a technical interface between the information system and the user. Via this interface, the user can control the user representation.

The *service-provider representation* is the internal representation of the agency or business from whom the user procures a service. The service-provider representation within the information system represents the person responsible for the system (e.g. the owner) and promotes the interests of the organization it represents. A key functionality of the service-provider representation is to control access to services. A service-provider representation can also collectively represent several businesses or organizations.

Services should be understood in the broadest sense. In many cases, these services will consist of information or information processing. Examples of services are: teletext and other databases for information collection, reading and writing of documents on a computer network, communication services, payments, etc. A service can also be a link to another (external) information system.

A *database* is the information system's internal (electronic) administration and contains the data required for the information system to function. The database controls the information system and is therefore not considered a service. Simple information systems do not even require a database; an example of such a service is teletext.

The database consists of two files: a *privileges* file and an *audit* file. The privileges file contains the users' privileges (equivalent to those of the user representation). The service-provider representation checks in the privileges file whether or not the user is authorized to access the various the information system's various services. The audit file records the use of the information system and can be used to charge the user for the use of an information system, or, for instance, to check when, why and by whom an information system has been used.

Each element of the model may be partially outside the (computerized) information system. All elements of the information system can interface with the system's environment, as outlined in Section 2.1. An audit file could be printed on paper. A user representation could take the form of a smart-card.

Each line connecting two elements of the model is an interaction line. Adjacent elements can generate an interaction across that line, e.g. data exchange. Thus each interaction line poses a potential threat to user's privacy since identifying data can be spread through the system by each of these lines. The elements will generally interact as part of a process initiated when the information system is used. In order to determine whether the person's identity is required for these processes, the processes carried out within an information system and their functions within the system as a whole must be clarified.

2.3.2 *Processes in the information system*

Use of an information system entails a number of processes: authorization, identification and authentication, access control, auditing and accounting. A process is an exchange of information between two or more elements within the information system, as indicated in the preceding section. Interaction lines connecting the elements are used for data exchange. The processes can take place independently of each other, with one process utilizing data generated by another process. Figure 2.2 shows the relationship between these processes. The processes of identification and authentication, access control and auditing take place entirely within the information system. The authorization and accounting processes have an interface with the environment.

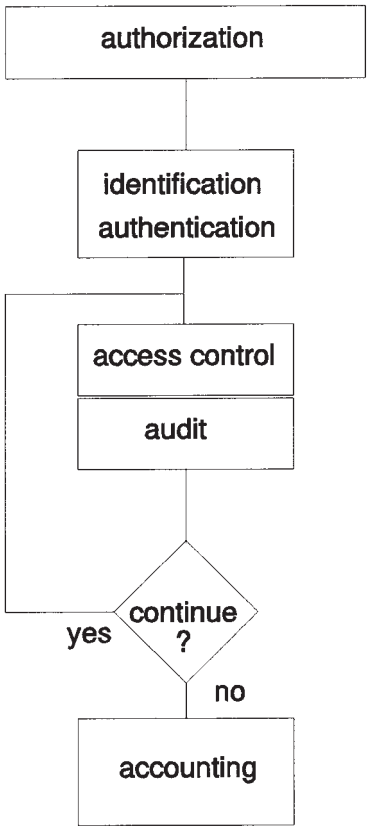

Figure 2.2: A possible order of processes in an information system.

Authorization is the allotment of privileges to the user. Before a user can use an information system for the first time, the service-provider determines the user's privileges and files this information in a database. User privileges are determined on the basis of user characteristics. The user is subsequently assigned a user representation within the information system. The service-provider representation links the user's privileges with his internal representation. A bank account number is a well-known example of internal representation.

The process of *identification* and *authentication* of a user representation is carried out when a user wishes to gain access to the information system via a user representation. In most information systems, the user introduces himself to the service-provider (identification), and then the service-provider checks the user's identity (authentication). The user uses the interface that is part of the user representation for identification and authentication. A common method of identification is to enter a user ID, although even the possession of a bank card can be considered identification. Authentication then takes place when a password or, in the case of the bank card, personal identification number (PIN) is entered.

Access control is a continuous process. The service-provider representation checks whether the user representation is authorized for each service provided. In this way, the service-provider representation prevents unauthorized use of services.

Auditing is also a continuous process. The service-provider representation can keep track of data pertaining to a service provided to a user's representation, registering, for example, which services have been used and for how long. This information, called audit data, is saved in the database's audit file. The service-provider decides which data the audit file is to record. Telephone units used to determine the cost of a call is one example of audit data.

In the *accounting* process, the service-provider charges the user for (trans)actions. Say the user has to pay for a service. The service-provider charges for use on the basis of audit data. Accounting generally takes place after the service has been used. However, accounting can also take place while a service is being used. The information system can, for instance, undertake direct action once the audit process sets off an alarm. An example is when a person trying to make an electronic payment types in the wrong PIN representation several times and the system cuts off the transaction or even "swallows" the card.

2.3.3 Need for identification within the information system

In the conventional information system, the user's identity is often needed to perform the processes outlined in the preceding section. Identity is used within the authorization process, for instance, to identify and record a user's privileges and duties. The user's identity is thus introduced into the information system. Since all of the various elements of the information system are involved in the five processes (in conventional information systems), the user's identity travels throughout the information system. Figure 2.3 illustrates which elements are involved in the various processes.

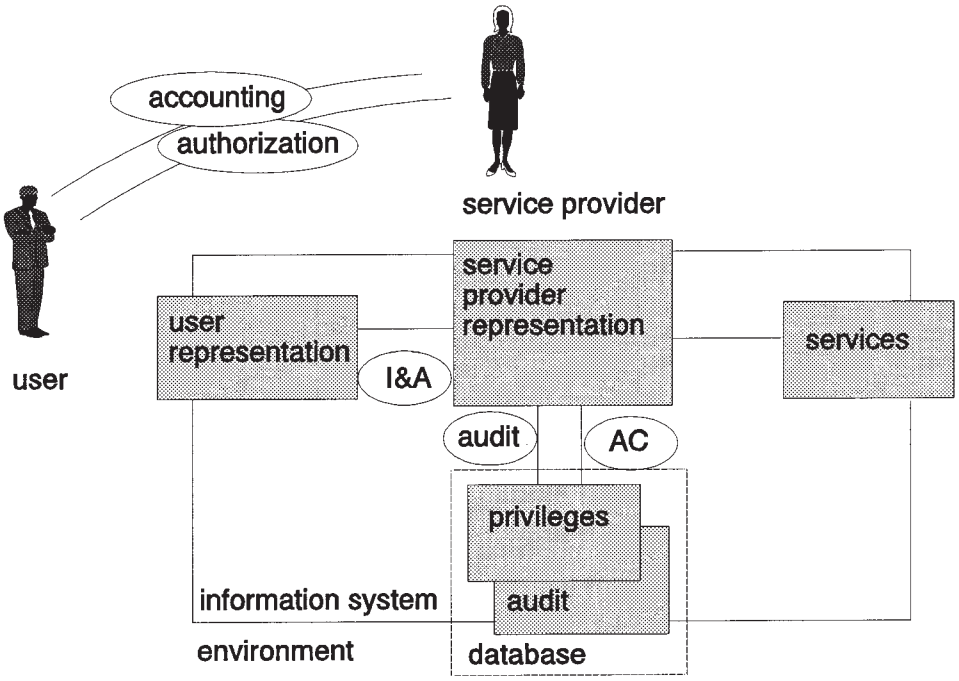

Figure 2.3: The relationship between processes and elements. (I&A: identification and authorization, AC access control)

For each of the mentioned processes, the question can be asked whether the user's identity is really required.

Is identity necessary for authorization?
In the authorization process, the service-provider assigns privileges to a (future) user. Whether identity is required for authorization depends on the manner in which the service-provider determines the user's privileges. If the service-provider wants to assign privileges on the basis of individual characteristics, then the user is required to demonstrate those characteristics. If privileges are given on the basis of a group characteristic, demonstrating this one characteristic suffices. A few characteristics include:

1. The user (known to the service-provider by a pseudo-identity) begins with limited privileges and accrues more over the course of time (depending on his behaviour). Take the no-claims bonus system for automobile insurance, for example. For each year the driver does not submit any insurance claims, he receives a discount on his premium. The accrual of no-claim benefits is comparable with the accrual of rights.

2. The user receives privileges by being a member of a group. The user must be able to demonstrate that he belongs to the group, club or association. Hotel guests gain access to hotel facilities like swimming pools, fitness rooms and parking places when they show their key.

3. Someone or something serves as a guarantor (trusted third party). Based on pledges made by this trusted third party, the service-provider can grant privileges on the basis of specific (individual) characteristics. One example is parking permits for the handicapped - a hospital can state that the patient, known by a pseudo-identity, does in fact have a handicap.

4. Privileges based on those obtained elsewhere, for example, transfer of privileges from another pseudo-identity. Employees can register for their employer's pension fund under a pseudo-identity. If the employee switches employers, the employee's rights - in the form of the premium paid - can be carried over to the new pension fund. The employee can then adopt a new pseudo-identity for these pension rights.

5. Privileges based on personal characteristics, for instance, age. All people 65 or older can travel for half price. The local authorities can issue a statement to this effect.

It is possible, however, that another information system must be used in order to verify certain characteristics required by a privacy information system. If this information system is a conventional one, i.e. one which uses the user's identity, the identity of the user will in effect be known to the privacy information system as well. A case in point is when a person requesting a visa has to show his passport as proof of nationality.
Conclusion: In most cases, it is not necessary to know the user's identity in order to grant privileges. However, there are some situations in which the user must reveal his identity to allow verification of certain required characteristics.

Is information about the user's identity necessary for identification and authentication?
In many cases, the authorized user receives an internal representation he can use within the information system. The user can then identify himself with his internal representation. Depending on the choice of internal representation and how well-known the representation is, it may or may not be possible to determine the user's identity on the basis of the internal representation. But by constantly changing the user representation, it becomes more difficult to link representation and user.
Conclusion: Information about the user's identity is not necessary for identification and authentication.

Is identity necessary for access control?
The access control process checks whether the user representation authorizes the user to perform certain activities. This process takes place within the information system. The internal representation of the user can be used as a reference in lieu of the user's identity.
Conclusion: The user's identity is not necessary for access control.

Is identity necessary for the auditing process?
Internal representation of the user also suffices for the auditing process. After all, it is only necessary to record what a (random) user representation does, so the user's identity is superfluous.
Conclusion: Identity is not necessary for auditing.

Is identity necessary for accounting?
As long as the user follows the rules, his identity need not be revealed. However, it may be necessary to know a user's identity when he has to be billed for the use of the information system. This can be the case, for instance, if the user misuses or improperly uses the information system and must personally account for it.
Conclusion: Identity is necessary for accounting in certain cases.

On the basis of the above analyses, the conclusion can be drawn that it may be necessary, in certain cases, to know the user's identity for accounting and authorization purposes. The necessity depends on the relationships that exist between the privacy information system and the environment. This situation arises if, in the environment of the privacy information system, a conventional information

system requests the user's identity. For the processes of identification and authentication, access control and auditing, which take place within the information system, knowledge of the user's identity is unnecessary. Figure 2.4 indicates which processes involve the use of identity, both in conventional and privacy information systems.

Process	Is identity used in a *conventional system?*	Is identity used in a *privacy system?*
Authorization	Yes	Sometimes (1)
Identification & authentication	Yes	No
Access control	Yes	No
Audit	Yes	No
Accounting	Yes	Sometimes (2)

Figure 2.4: The use of identity in conventional and privacy information systems. (1) In certain cases a consumer must appeal to conventional information systems, which uses the user's identity. (2) In certain cases the user must personally account for it.

3 Identity domains

This chapter illustrates how privacy techniques can be used to separate the user's identity from the use of the information system. A number of these techniques are given in the literature (Chaum, D., 1992). Based on the model of the information system presented in Chapter 3, a description will be given of how the information systems can be structured in order to better protect the privacy of the user. Section 3.1 will introduce a new system element designed for this purpose: the identity protector. The technical set-up of this identity protector depends on the specific information system. Appendices A to D describe a number of concrete applications.

3.1 The identity protector

The identity protector can be seen as a system element that controls the exchange of the identity between the other system elements. The identity protector is installed, quite logically, on one of the interaction lines in the information system. This means the user's identity can no longer be spread to the cordoned-off area of the information system. The role of the identity protector is comparable to that of the service-provider representation in the information system; whereas this protects the interests of the service-providing organization by e.g. monitoring access of users to the services, the identity protector protects the interests of the user - specifically, it screens dissemination of his identity. Just as the service-provider wishes to protect his services, the user wishes to protect his identity.

An important functionality of the identity protector is conversion of a user's identity into a pseudo-identity. The pseudo-identity is an alternate (digital) identity that the user may adopt when using the system. Examples of pseudo-identities in conventional information systems include account numbers at banks and social security numbers for the tax authorities. In the conventional and future information systems, the identity protector may take the form of, say, a separate functionality within the information system, a separate information system controlled by the user (e.g. smart-card), or another information system that is under the supervision of a third party trusted by the service-provider and the user.

The identity protector offers the following functions:

- reports and controls instances when identity is revealed
- generates pseudo-identities
- translates pseudo-identities into identities and vice versa
- converts pseudo-identities into other pseudo-identities
- combats misuse.

The user can set the identity protector for certain purposes, for instance so that his identity is kept entirely confidential when the system is used legitimately. Another possibility is for the user to set the identity protector to reveal his identity only to certain service-providers.

Integration of an identity protector creates two domains within the information system: one in which the user's identity is known or accessible, and one or more in which it is not. The term *identity domain* denotes the domain in which the user's identity is known, the domains in which the user's identity is secret are termed *pseudo-domains* (see figure 3.1).

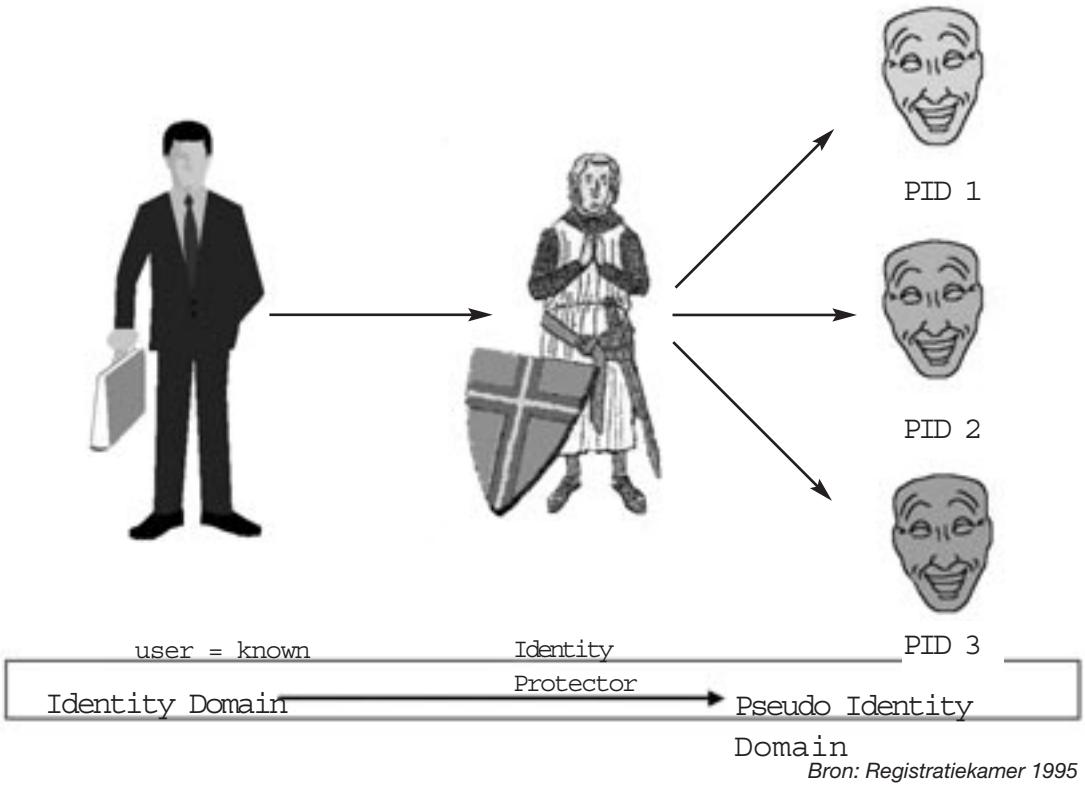

Figure 3.1: The identity protector separates the identity and pseudo domains.

The user must be able to trust the way his personal data is handled in the domain where his identity is known. The identity protector can be placed anywhere in the system where personal data is exchanged. A simple guideline for the designer of a new information system is to minimize the identity domain. Depending on the elements within the information system that can be trusted (in terms of privacy protection), a number of configurations of a privacy information system can be distinguished. The following section describes a number of these configurations in which the user's identity is unlinked from parts of the information system.

3.2 Cordoning off areas of services and other users

The services element of an information system can be structured in such as a way that the privacy of the user is not adequately protected. By placing identity protectors between the services and the other elements of the information system, privacy protection can be improved. This means services are located in the pseudo-domain, while other elements remain in the identity domain (see figure 3.2).

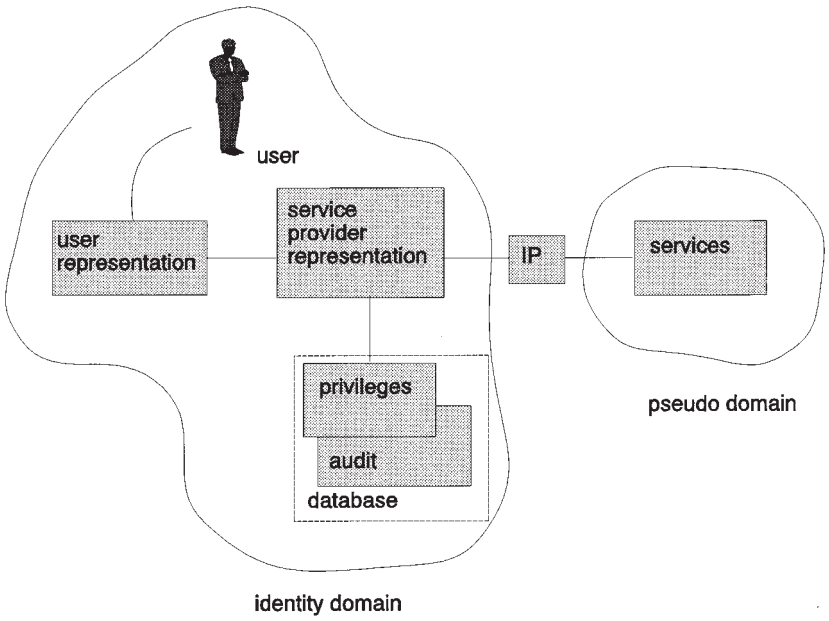

Figure 3.2: An identity protector protects the privacy of a service user.

When an identity protector is integrated into a system, the user can use services anonymously, not only increasing privacy in terms of that particular service, but in relation to other users. This last aspect is especially relevant to communication services. Several users can generally use the communication services offered. A communication system such as a data network is an information system intended for use by many people. In many cases involving an information system with multiple users, the identity of users can easily be kept confidential from fellow users. A condition is that service-providers take measures such as furnishing the information system with an identity protector, or the functions corresponding with one.

The following two examples illustrate the point. The first example is a direct extension of the communication system and illustrates a situation in which both services and other users are cordoned off. In the second example, only a service is cordoned off.

Example 1. In the regular analogue telephone networks, a caller has long been anonymous to the person receiving the call. The person on the receiving end could not identify the calling party before deciding to answer the call. Digital telephone networks now enable the receiving telephone to display the number of the person calling. With the help of suitable peripheral equipment, the displayed telephone number can also be saved and coupled to stored data files (Registratiekamer, 1994). The function allowing the caller's number to be displayed is termed Calling Line Identification. This function offers the caller a number of possibilities for blocking his number so it is not revealed: the calling line number is not displayed at the receiving end (PTT Telecom, 1993). Appendix A provides further information on *Calling Line Identification*.

Example 2. Sometimes users do not have direct access to an (international) network, such as Internet, but need an intermediary information system to gain access to the system and its services. In the case of Internet, this is done via an Internet server. This kind of information not only acts as an intermediary, it can also act as a representative of the user: the users are given a temporary pseudo-identity with which they can use the services the network offers.

3.3 Protection of registration in the database

A service-provider's database consists of a privileges file and an audit file. The privileges file contains the users' privileges and the audit file contains all the other information the service-provider has recorded for provision of his services. Since these two files may register personal data, this system element merits the special attention of the privacy-conscious designer.
The identity protector makes it easy for the designer to minimize the personal data filed in the database. In effect, the service-provider does not register the user's privileges and/or actions under his real identity, but under a pseudo-identity. Figure 3.3 presents a situation in which both the privileges file and the audit file are included in the pseudo-domain. It is also possible to cordon off one of the two files.

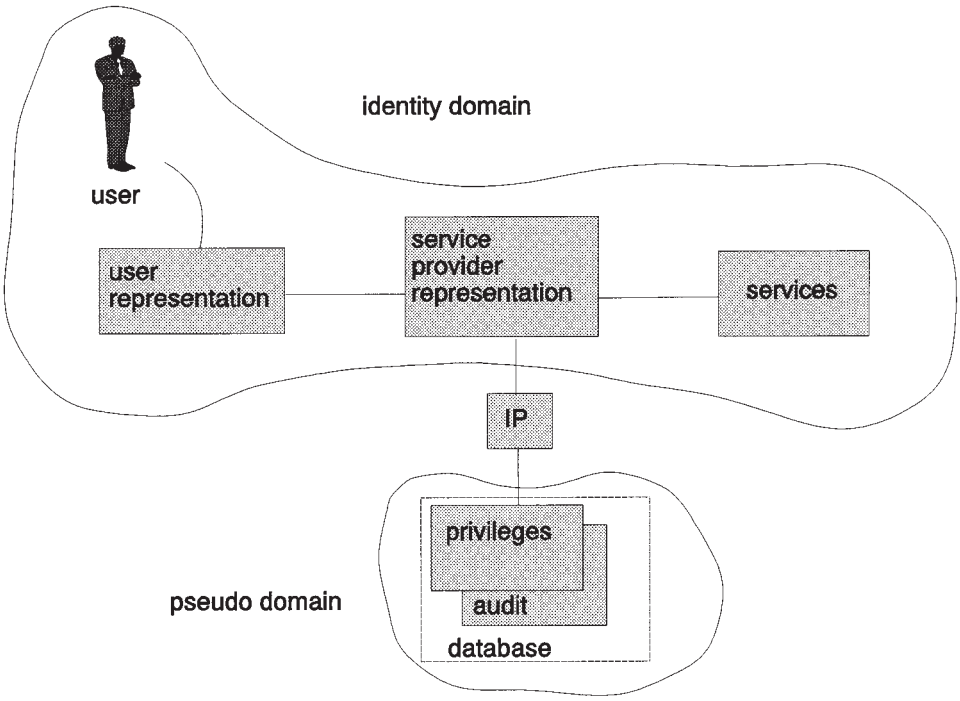

Figure 3.3: An identity protector prevents the registration of the user's real identity in the data-bases (the privileges and the audit file).

Appendix B describes a system for the provision of medical data. In the following example, the audit file of a call-center is included in the pseudo-domain.

Example: A large business starts using a *call-center*, a telephone exchange linked to a computer system, which directs internal and external telephone and data traffic. The telephone numbers of all the calling and receiving lines and the duration of calls are registered for all outgoing telephone calls and external data services (for internal charging and capacity and waiting time statistics). Not the name of the caller or employee making an outgoing telephone call is recorded, but a code that changes daily. This daily representation is generated by a *reliable* network function: the identity protector. This does not detract from the possibilities of making statistical calculations of capacity and waiting times. Costs can be charged internally because the system keeps records of the cumulative data per department.

3.4 Cordoning off the entire information system

By placing the identity protector between the user representation and that of the service-provider, a pseudo-domain emerges which envelops the services, service-provider's database, and the service-provider representation itself (see figure 3.4).

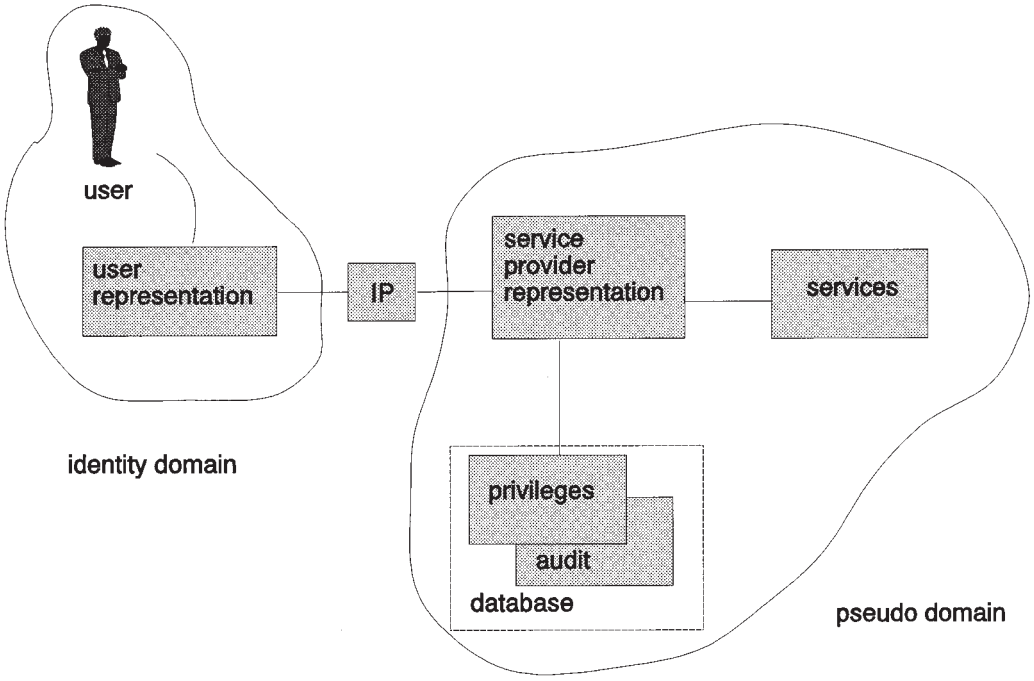

Figure 3.4: Cordoning off the entire information system.

In this situation, the identity domain only contains the user representation. This is also the only part of the information system that the user must trust. Less stringent privacy protection requirements can be set for the other system elements in the pseudo-domain. When installing an identity protector, it is important that the way in which communication between the user representation and the service-provider representation be clearly defined and sufficiently secured against intrusion from third parties. User trust in the user representation can be gained if the service-provider takes stringent security measures, or if users have access to and control over a user representation that they can set themselves. This can be a portable computer or a smart-card.

An important aspect of this configuration is that the service-provider must be able to determine what the user is authorized to do, without learning the user's identity. There are various different possibilities for authorizing the user. Section 2.3.3 describes a few situations.

Within the configuration, the identity protector acts as a sort of intermediary for the processes both the user and service-provider go through. So both parties must be able to trust the identity protector. Techniques that are suitable for use with a trusted third party (who could be called a digital attorney) are also suitable for an identity protector in this situation.

Example: A new employee of a large organization must be given access to the corporate network. The systems manager has to set up a directory and the authorizations in accordance with the employee's access profile, which is strictly confidential. The access profile is drawn up by the head

of the department on the basis of the required access level. The profile, not containing data that can be associated with the new employee, is sent to the systems manager, who checks the profile for authenticity, implements the authorizations and then returns the request form to the department head. The systems manager has added a user ID number and password to the form. The new employee now has access to the network without the systems manager knowing who the employee is. If the employee does something he is unauthorized to do, he can be identified through the department head. It is important that both the systems manager and the employee trust the department head.

3.5 Situations with several service-providers

In many cases, several service-providers are involved in the provision of services: it is only possible to pay with a bank card, for instance, if the bank and shopkeeper work together and construct their information systems to accommodate it. Situations involving several service-providers can be complex, and adding an identity protector to a common or linked information system can create specific problems.

A common situation is when two service-providers, let us say A and B, both provide a service to a user, whereby service-provider A supplies a primary service and B a secondary service. Take the bank card example: the shopkeeper supplies a primary service and the bank a secondary service. In this case, the user's privileges are recorded at the secondary service-provider. Figure 3.5 presents a diagram of this situation.

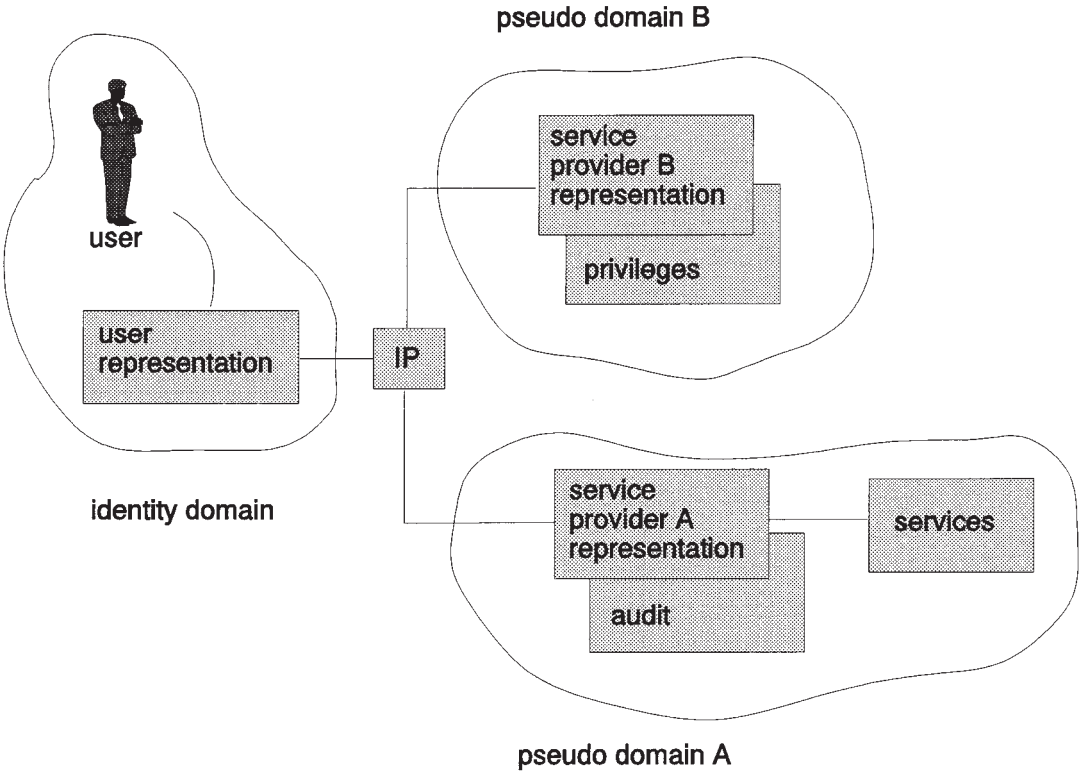

Figure 3.5: Two service providers in different pseudo-domains.

Service-provider A verifies the user's privileges at/through service-provider B. The identity protector can be installed as two separate functions: one function for each separate service-provider, or as one function for both. This function can be integrated into a smart-card, for instance, that the user carries in his pocket.

It is even possible to integrate a service-provider with the user's representation. Service-provider B can mark an electronic document and give it to the user. Then service-provider A can determine what the user's privileges are by verifying service-provider B's mark on the electronic document. Figure 3.6 shows this situation. In this situation, too, service-provider A determines the user's privileges by checking with service-provider B.

An information system arranged in such a way that the user carries his privileges with him is comparable to an ambassador carrying a *Letter of Credence*. In the literature, privileges granted in this manner are termed *credentials*. Credentials can be compared with certificates issued by one agency and valid when presented to other agencies. The term credentials will be used throughout the rest of this report to denote privileges that the user carries.

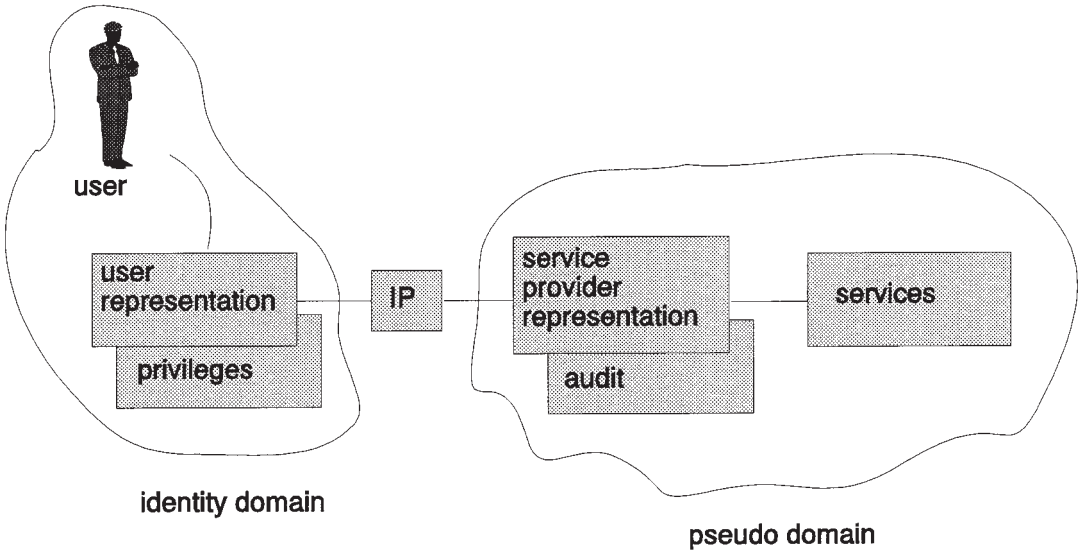

Figure 3.6: The user carries his privileges with him.

The following examples demonstrate that the service-provider does not need to know a user's identity in order to provide services. The first two examples illustrate anonymous payment. The third example describes an interaction between a hospital and an insurance company. When the patient comes in for a certain treatment, his privileges (e.g. insurance policy) are checked without the patient's name being revealed to either the hospital or insurance company.

Example 1. Payment transactions, in which the account number serves as the pseudo-identity and a trusted third party is the only one, besides the user himself, who knows the relationship between the account numbers and the identity of the account-holder. In this case, the identity of the account-holder corresponds with his name, address and town of residence. The trusted third party must also send mail for the bank, since the bank does not have any addresses. The trusted third party could be an independent agency or a part or department of the bank itself: in that case, the service-provider enters only a small part of the identity domain, i.e. that part in which mail is sent.

Example 2. Users have an electronic wallet, provided at no charge by the bank, with digital cash. Users can deposit a maximum amount of money in the electronic wallet, for instance by depositing real cash. The digital cash is actually a number representing an amount, which is sealed with a bank identification mark. The shop-keeper also has a digital wallet. The bank can transfer the digital cash from one wallet to another by calculating the new total amounts and sealing these with the bank's digital mark. Appendix D provides further information in the use of digital cash.

Example 3. The service-provider, say a hospital or doctor, wants to check whether a patient is insured for a particular treatment. The hospital and the insurance company know the patient by different pseudo-identities. Via the identity protector, which can translate pseudo-identities, the hospital can determine what coverage the patient has for which treatments.

3.6 Fraud prevention

The identity protector should also prevent fraud or improper use by the user. This can take various forms, such as prevention, detection and correction. One possibility is for the identity protector to prevent the user from being able to use his anonymity to commit fraud. Another approach is based on a combination of detection and correction. The identity protector can determine which measures can be taken *against* the user, such as revealing his identity to the service-provider involved or to the authorities (e.g. police). The set-up of the identity protector should also make it possible to inform the user that his identity is to be revealed.

Examples of preventive methods to keep people from taking improper advantage of their anonymity include hospital insurance cards and (digital) cash. Authentication through entrance representations or biometric data (e.g. fingerprints) renders it impossible for someone else to use a health insurance card. Paper bills are generally made difficult to counterfeit through the use of water-marks and special types of paper and ink in the production process. The same principles hold for digital cash. Cryptographic techniques can be used to prevent one sum of cash from being spent anonymously more than once.

In this example, an identity protector detects a user trying to take unfair advantage of his anonymity and corrects the user: a user receives access to a certain service through the mediation of a go-between (such as a *digital* attorney) which acts as an identity protector. The service-provider wants to charge the user for the service provided and sends the bill to the intermediary, who, in turn, sends the bill to the user. If the user does not pay, the service-provider will eventually ask the intermediary for payment again. There are now several ways in which the intermediary can approach the user. He can use cryptographic techniques to reveal the user's identity to the service-provider. The service-provider can then contact the user directly or through a collection agency. Another option is for the intermediary to seek contact directly or through a collection agency in order to secure the user's payment. However, the user should always be given the chance to prove he has been falsely accused of misconduct before his identity is revealed.

4 Implementation Techniques

Are the models we presented in the previous chapter feasible? This chapter begins with an explanation of some specific techniques for integrating an identity protector into a system and concludes with some guidelines for the development of privacy-protecting information systems.

4.1 Setting up an identity protector

So far this report has presented the identity protector as an abstract functionality, or black box, which places the designer in a position to construct the information system so that the user's identity is cordoned off and only revealed in certain situations. The designer is not limited in his choice of special techniques for the creation and implementation of the identity protector. Some techniques, such as digital signatures and trusted third parties, merit special attention.

4.1.1 Digital signatures

A signature or wax seal on a document is proof of its *authenticity*. A digital signature is an electronic version of a hand-written signature. The key aspects of both types of signatures are that only one person or service-provider is capable of producing the signature, and all others are capable of verifying it (see figure 4.1).

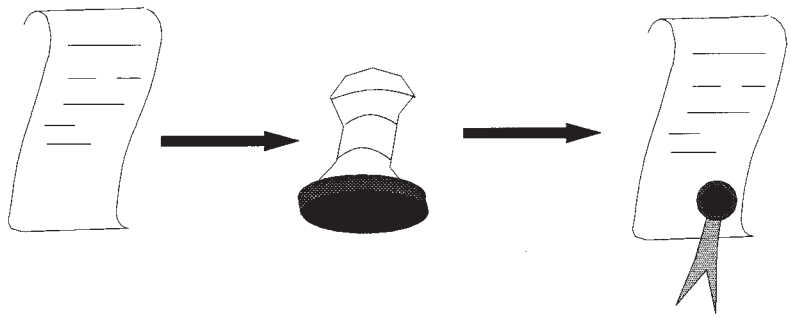

Figure 4.1: A digital signature corresponds with a written signature or a wax seal. A signature on a document is proof of its authenticity.

How is a digital signature made? In most cases, digital signatures are created by means of an irreversible process within the electronic document that calculates a digital value. This value is called the hash or *compaction* value. The purpose of the hash value is to convert a random electronic document into a digital value of a fixed length (in bits). This simplifies the application of cryptographic techniques, used to encipher the hash value into numbers. The result is a digital signature, which can be distributed together with the electronic document.

The signature, i.e. proof of a document's authenticity, can be validated as follows. The sender and recipient make agreements concerning the enciphering method and irreversible process, which enables the recipient to calculate the document's hash value. The digital signature is deciphered cryptographically. The recipient now has two values he can compare. If the values match, the file received is authentic, if they differ, the file has been altered in transit. This could be due to tampering or because of a transmission error.

Everyone who has an agreement with the person compiling the document (sender) can verify that the electronic document is authentic by checking the corresponding signature. Digital signatures are only valid for the electronic document for which they were created. Each electronic document has its own (unique) digital signature.

A potential application of digital signatures is digital driver's licenses. The issuing authority could attach a digital signature to an electronic document which holds the class of the permit. Other organizations like car rental companies and the police can then check the driver's credentials by screening the digital signature on the electronic driver's license.

4.1.2 Blind digital signature

A blind digital signature is a special kind of digital signature (Chaum, D., 1990). The difference does not lie in the signature itself, but in the document to which it is attached. When a person places a regular digital signature on a document, he is familiar with the contents of that document. A person placing a blind digital signature, on the other hand, has no or only partial knowledge of the document's contents. The signer often has a certain authority or represents a certain agency, such as a notary, and is not accountable for the document's contents.

A blind signature works like this: a user brings a document to a notary. The user does not want anyone, including the notary, to know the contents of the document. The user seals the document in an envelope. A portion of the document is visible through the envelope. The notary places a wax seal on the visible portion. The seal is proof of the document's authenticity. When a blind digital signature is used, cryptographic techniques replace the envelope and wax seal. The user enciphers the digital document, which is comparable to putting the document in an envelope. The notary places a digital signature on the document in the envelope (see 4.1.1). When the document must be checked for authenticity, the signature is validated.

The document can be represented as an electronic letter and envelope. Figure 4.2 schematically illustrates the cryptographic process.

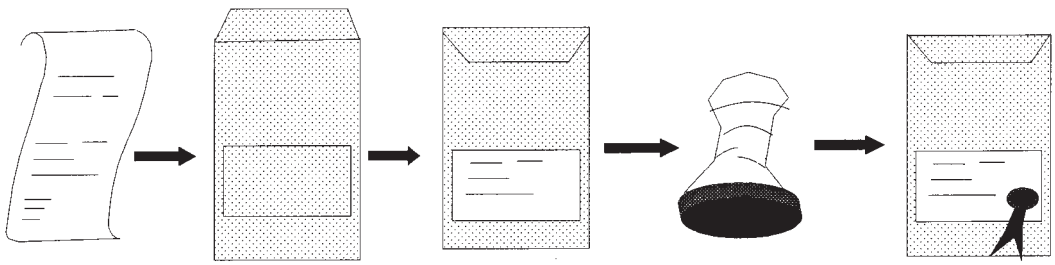

Figure 4.2: A blind digital signature: The digital envelope protects the contents of the digital letter. The digital signature on the letter is proof of its authenticity.

An application involving blind digital signatures is *digital cash* (Chaum, D., 1992). A user takes an envelope to the bank. The envelope states the user's account number and contains a piece of carbon paper and a bill. The user asks the bank to assign a value of 10 dollars to the bill. The bank places an official stamp on the envelope to give it the value of 10 dollars (blind digital signature). The bank uses a different stamp for every value. The stamp is copied onto the bill through the carbon paper. Now the user can remove the bill from the envelope and he has a 10-dollar bill. The bank cannot link the bill to the user's account number and thus to his identity. When the user spends the bill, neither the bank nor the service-provider receiving the bill as payment can draw a connection between the bill and the user. The service-provider can tell from the stamp whether the bill is real.

4.1.3 Digital pseudonym

A digital pseudonym can be represented by a completely random selection of characters (letters, numbers and punctuation marks). The user is not known to a service-provider by his identity, but by this series of characters. He can select a *different* pseudonym for *every* service-provider. Consequently, service-providers cannot exchange information about individual users. A different pseudonym can also be used for each service or individual time a service is used.

If there are n service-providers, the user chooses n pseudonyms: PID-1, PID-2, up to PID-n. The *ith* service-provider knows the user by the pseudonym PID-i. The service-provider assigns privileges to this pseudonym by furnishing a blind digital signature. The user keeps the assigned privileges and can use these privileges with other service-providers under a different pseudonym.

Users have a special *envelope* with a transparent window for each service-provider, which enables them to communicate with service-providers. The user - or a third party in whom he trusts - collates all these pseudonyms in one digital letter. Service-providers can give users new privileges by adding blind digital signatures, a signature corresponds with a specific privilege. The user can present other service-providers with proof that he is (properly) authorized (see figure 4.3).

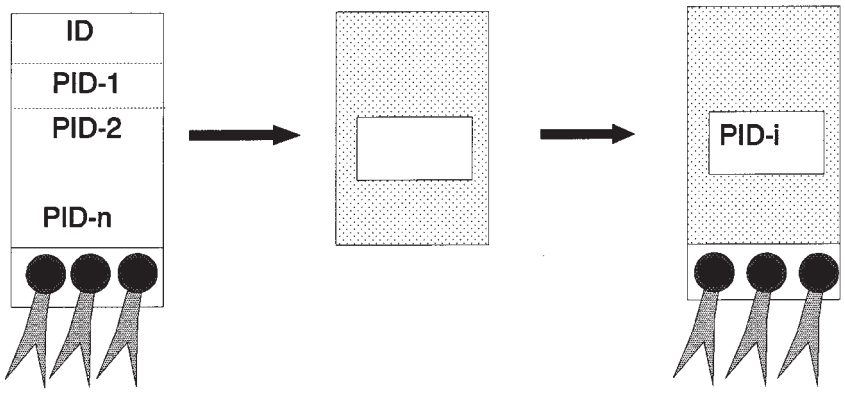

Figure 4.3: Digital pseudonyms offers a user the possibility to present proof of his privileges under different pseudo-identities. The user has for this purpose a number of digital envelopes with a transparent window.

The user can also use obtain services from service-providers without a pseudo-domain provided he reveals his identity. The user then presents proof of his identity and the digital signatures he has obtained.

Digital pseudonyms can also be used for the digital driver's license mentioned in Section 4.1.1 above. Here, the issuing authority has given the driver a blind signature which corresponds with a pseudonym, using a digital signature for each class of license. The driver can use a different pseudonym to prove (e.g. to a car rental company) that he is authorized to drive certain vehicles, by presenting the digital signature(s) he received from the issuer.

4.1.4 Trusted third parties

A trusted third party is a term for a service-provider who is trusted by both *users* and *service-providers* (a sort of digital attorney). The trusted third party can, for instance, keep track of the digital pseudonyms a user uses in his relationships with a number of service-providers (see figure 4.4).

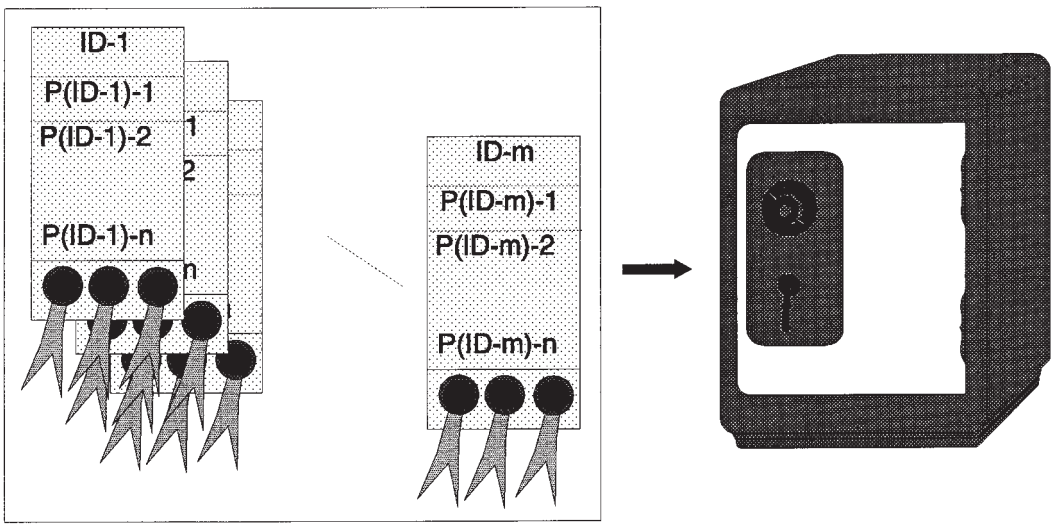

Figure 4.4: A trusted third party can keep track of the digital pseudonyms a user uses in his relationships with a number of service-providers.

The user's trust is founded on the discretion the trusted third party observes with respect to his identity: the trusted third party must keep the *relationship* between the *identity* and *pseudo-identities* secret. The service-provider's trust, on the other hand, is based on the assumption that - if conditions require - the trusted third party will reveal the user's identity. A service-provider may need the identity of a user in order to hold the user accountable for wrongful or improper use. After the user has accounted for his actions, he can initiate a new relationship, under a different pseudo-identity, with the service-provider.

In the above example of digital driver's licenses, a trusted third party can register and keep track of the relationship between the driver's identity and the pseudo-identities stated on his license. In certain cases, a driver's identity can still be determined on the basis of his pseudo-identities. These powers should be reserved for organizations like law enforcement agencies.

4.2 From conventional to privacy information system

When a new information system is being engineered, or a conventional information system is being upgraded, the client, designer, developer or supplier of an information system can ask himself how the user's privacy can be better protected.

In the analysis phase, the question should be asked how much and which personal data is required for the information system to function properly. An attempt must be made to *minimize* the amount of information, particularly identifying data, filed by an information system. Minimization of data has implications for information system processes of input and output and the ways in which a system records information.

The position of the identity protector - or an equivalent functionality - within the information system *is a crucial part of the design phase*. A decision has to be made about which elements should belong to the pseudo-domain and which to the identity domain. This is also the phase in which to determine how the user is to exert control over release of his personal data. This is a matter of how the identity protector is to be set up. What are the identity protector's functions to be?

Questions concerning specific techniques for creating the identity protector arise in the *implementation phase*. The issue of concern is that the information system must not allow data to circumvent the identity protector and thus *leak* from the identity domain into the pseudo-domain. Special attention must be paid to what could be unique serial or production numbers generated *automatically* by hardware and software.

Figure 4.5 indicates how the designer can take the user's privacy into account during the different phases of the design process.

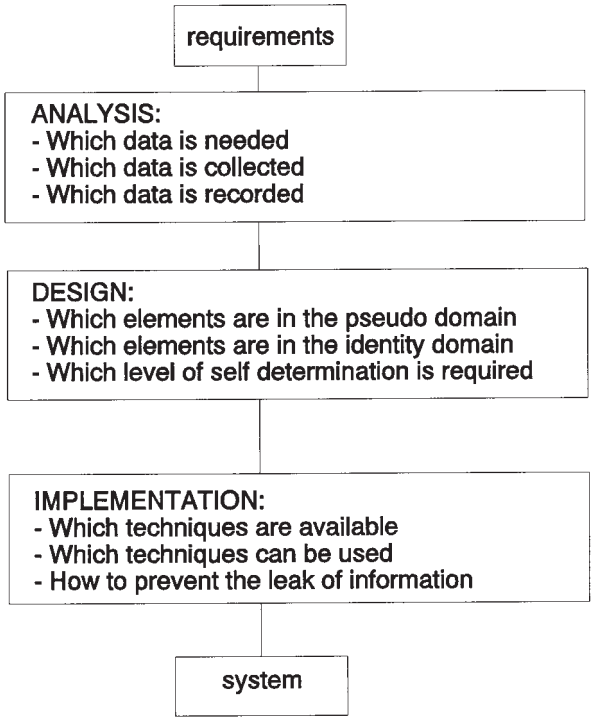

Figure 4.5: Aspects to take into account during the different phases of the design process of a privacy information system.

Appendix A: Calling Line Identification (CLI)

A digital telephone network enables the receiving party to identify the caller via the telephone number: the network communicates the number to his telephone or other peripheral equipment. This number can be directly displayed or used as a search key within a database so that other data pertaining to the caller is retrieved. This function is knows as *Calling Line Identification (CLI).*

To date, the service-provider in Figure A.1 (the telephone company in this case) still requires the caller's identity in order to charge him for the services provided. This means it is not (yet) possible for the caller to remain anonymous to the service-provider. The person receiving the call in Figure A.1 is another user of the information system who can be approached via the service of *phoning.*

The caller can keep his identity secret through the use of an identity protector, which consists of a number of blocking options integrated in the functionality of the Calling Line Identification. In CLI, the caller can determine whether his telephone number is to be revealed. CLI thus offers the functionality of an identity protector. Here, the identity protector is located between the service-provider and the services (see figure A.1).

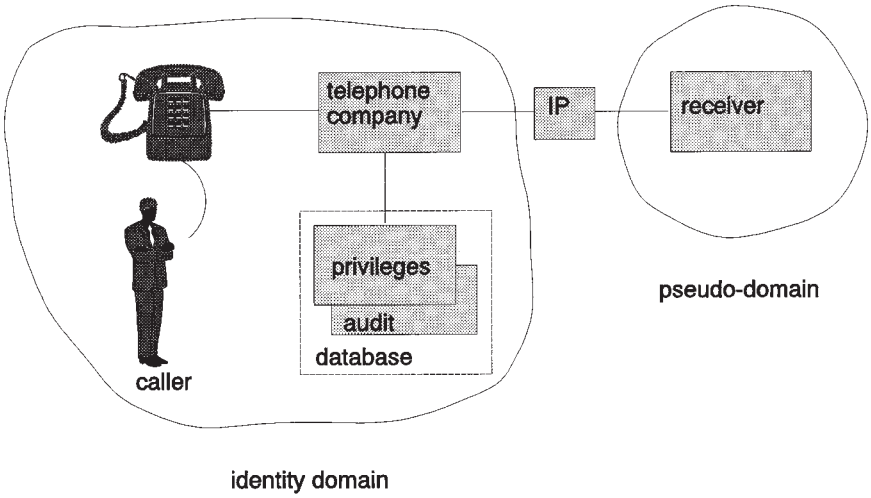

Figure A.1: The functionality of the Calling Line Identification can be compared to the functionality of an identity protector.

Blocking options offered by CLI

The caller has the option to block his number, so that the number of the calling line is not passed on to the receiving end (PTT Telecom, 1993). The different blocking possibilities offered by CLI include:

1. blocking CLI per call
2. total blocking of CLI.

Blocking CLI per call

If a code is entered before dialing the receiver's telephone number, the caller's telephone number is not displayed to the receiving party. This code is checked by the identity protector. The identity *protector* works in this case as a user-controlled filter for identifying information (telephone number).

Total blocking of CLI

It is arranged with the telephone company that the telephone number of the caller is never to be given to those on the receiving end. Here, the identity protector works as a pre-set fixed filter for the identifying information, i.e. the telephone number.

In addition to the caller's options to block display of his telephone number, there are ways to protect the one receiving a call from the caller. After all, the caller could be invading the privacy of the person he is calling. There are two possibilities:

- the receiver can decide that anonymous callers are not to be given access to his peripheral equipment. In this case, the caller does not know whether the receiver is out or just not taking his call.
- certain (governmental) agencies (such as those providing assistance) have the option to overrule the caller's choice to block his number for each call or all calls. This allows the receiver to obtain the number of the caller. The caller then receives a signal that, in spite of blocking, the receiver has been informed of the number.

Conclusion

Calling Line Identification and concomitant blocking options exemplify the function of the identity protector in a digital telephone network. The most important aspect of privacy protection with respect to CLI is that the caller can decide whether or not his number is to be given to the person receiving a call.

In addition, the person receiving calls can guard himself from unidentified callers by refusing to take calls when the number has been blocked. Sometimes, such as when calls are received by police and emergency hotlines, it may be advisable to overrule the blocking.

The way in which CLI works depends on the implementation within the network by the service provider. From the perspective of privacy, the telephone company would preferably make CLI blocking the standard, in which case the caller should be able to turn the standard blocking feature off by simply pressing a button. However, the current implementation by the dominant telecom operator in the Netherlands is such that a subscriber has to take extra action to block a number from being passed on. This could be technically circumvented by 'instructing' the telephone of the calling party to enter by default the blocking code before the number, and enabling a deblocking code on a case-by-case basis.

Appendix B: Provision of medical data

Every day, medical data concerning individuals is stored in databases. Medical information is not only important and interesting to the physician who treats the patient, but to many others like fellow doctors, nursing staff, pharmacists, insurance companies, scientific researchers, and employers. Databases where this information is filed often lack features to protect privacy, meaning that anyone who has access to these databases has access to all data on an individual patient (Rossum, H. van, 1994).

Not all involved parties need to know the patient's identity. Scientists conducting research into certain illnesses/trends, for example, do not need to know the identity of the person. What is important to them is that they have access to all the data relevant to a study. Not only the illnesses and treatments that a patient has gone through are of interest, but also certain habits, like smoking, exercise, etc. So far, scientists have used patients' identities in order to collate all of the registered information.

System description

There is a number of methods for protecting the patient's privacy when medical data is stored in a database. This appendix focuses on two options: one in which the patient has one pseudo-identity, and one in which the patient has a different pseudo-identity for every involved party or application, assuming in both cases that only authorized persons know the identity of the patient. The use of multiple pseudo-identities is illustrated with a description of a successful application within a hospital information system, the so-called privacy-incorporated database (Blarkom, G. van, 1998).

One pseudo-identity per patient

The doctor gives each patient a pseudo-identity. The doctor keeps the relationship between the identity and pseudo-identity of the patient secret. The doctor could, for instance, entrust the identity and corresponding pseudo-identity to a trusted third party. The doctor records the medical data on the patient under his pseudo-identity. Other parties can now have access to the database containing medical information without learning the patient's identity.

Multiple pseudo-identities per patient

A second method is based on multiple pseudo-identities per patient. These pseudo-identities can be stored together with the identity in files that are only accessible to the trusted third party. The pseudo-identity of a patient is different for each party 1, 2, ..., n (see figure B.1).
The doctor can assign the patient certain characteristics by including a digital signature with the patient's identity (ID). Say the patient is administered a certain medicine - the doctor places the signature corresponding with that medicine under the patient's identity. The other parties (i.e.

pharmacy, insurance company and researcher) can now determine whether a patient receives that particular medicine by checking for the corresponding signature under the pseudo-identity PID-1, PID-2, ..., PID-n.

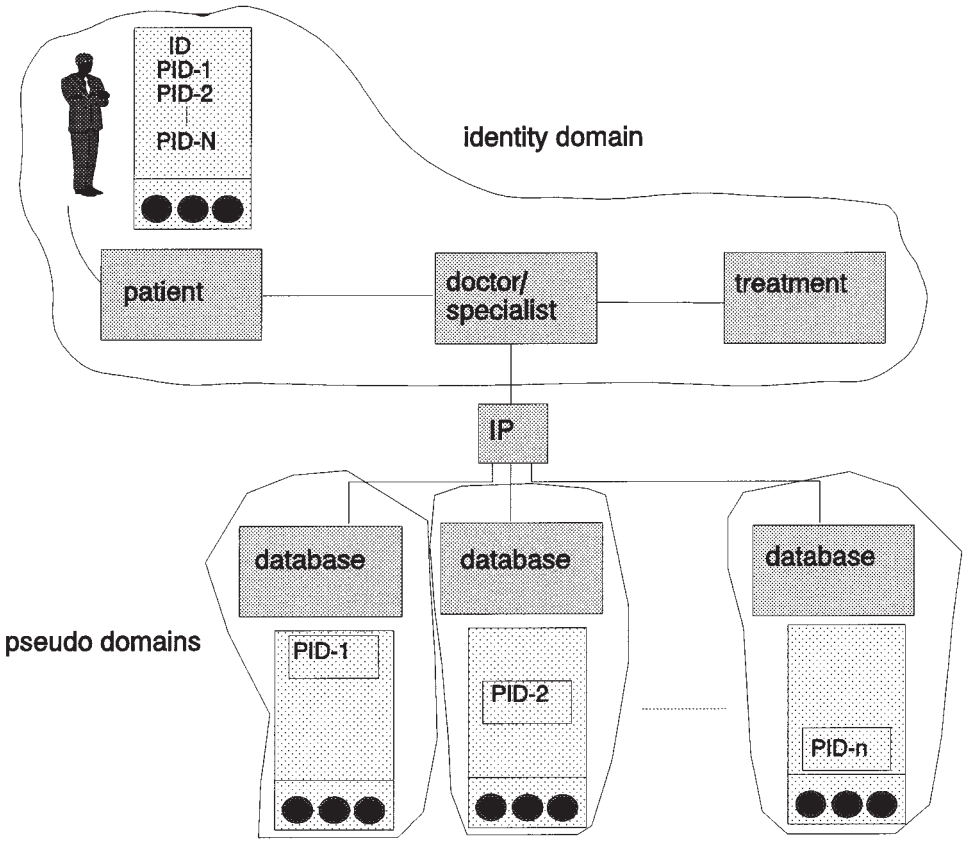

Figure B.1: Multiple pseudo-identities in the database. The different pseudo-identities cannot be associated with each other. So the patient can not be identified without the help of the identity protector.

Privacy-Incorporated Database

A successful practical application of multiple pseudo-identities can be found *within* a hospital information system (HIS).

In modern information systems, data is held in a relational database management system in units called tables. The data is split over a number of tables where each table contains logically related data items. In a typical HIS there would be a table named 'patient' holding the patient's personal details, a table named 'medication' holding the prescriptions, or a table named 'surgical treatment' holding the details of the operations performed. To each patient's name in the database a number is assigned to distinguish him or her uniquely. In order to link e.g. the medications and surgical treatments to the patient concerned, his unique database number is copied into those tables. It is obvious that a such database offers privacy risks:

1. once the patient's name is located, the database number is found and this value might be used to read the table 'medication' or 'surgical treatment' to find the medical records of the patient;
2. by searching any of the data in the linked tables, with a little deduction, the unique database number can easily be used to establish the identity of the patient.

A method has been developed for de-coupling the data tables in some instances, without losing the ability to maintain essential links.

The solution: The system is based on a client-server architecture. This means that the database is held on a central computer system (server). Each user accessing the application needs a personal computer (client). Application programs in the client issue database-access commands to read the data. The data is transferred from server to client, the data can be modified by the user and subsequently sent back to the server to modify the data in the database.

First the Identity Protector removes the patient-identifying number from all tables forming the medical record, and adds a data item for a pseudo identity. This pseudo-identity item is calculated from the patient-identifying number using an encryption technique. The program performing this encryption is executed within the client computer. The result is a database where each patient has a unique identifying number. In order to read the medical record, this number is encrypted to a value that can subsequently be used to access the medical record.

A typical process will look like this:
1. After successful log-in by a user at a PC-client, a process is started to select the patient whose medical record is to be accessed;
2. once the correct patient is identified, the unique identifying number is passed from the server to the client;
3. within the client computer, this number is encrypted, yielding a value which is used as the pseudo-identity of this patient; and
4. using this pseudo-identity, the required table(s) containing the medical record are accessed.

Because unauthorised users accessing the database can see no relation between the number and the pseudo-identity, the database is secured. Obviously, the encryption process can be reversed, to decrypt a pseudo-identity, resulting in the identifying number.

The implementation of the Privacy-Incorporated Database has no consequences visible to the users of the application. Both the identifying number and the pseudo identity are codes used inside the database. The user of the application will use an external identifying code, e.g. a social security number. The encryption is performed at no measurable cost within the client computer. The privacy-incorporated database has, therefore, no negative effect on the performance of the application.

Discussion

The first method, using one pseudo-identity, ensures that organizations have access to all data except the identity. However, all of this information could be used to link the pseudo-identity to the patient's actual identity. There is a chance that a single pseudo-identity can be associated with the patient's identity.

In the second method, the patient uses a different pseudo-identity for each agency or, within an information system, for each table in a database. In this case, the different pseudo-identities cannot be associated with each other, hence the risk that they will be traced to the identity is reduced.

Appendix C: Road-pricing

In the late eighties, the Dutch Ministry of Transport and Public Works considered introducing road-pricing. The purpose of this system was to charge road users for actual road use, as contrasted with customary road tax based on possession of a vehicle. The preferred method for a road-pricing system was one in which road users could pay automatically with a smart-card (Stoelhorst, H.J. en Zandbergen, A. J., 1990). Implementation of a road-pricing system in the Netherlands is foreseen for the first years of the next century (Tweede Kamer, 1997).

System description

There are two fundamentally different approaches to road-pricing: the first is a system in which the road user pays *afterwards* and the second in which this occurs *beforehand*. In the literature, these variants are referred to as post-paid and pre-paid systems.
The *post-paid* system can be simply achieved by requesting the vehicle registration number at the time the vehicle passes a toll point. The registration number is automatically called up. This system offers little or no protection of the road user's privacy - the vehicle registration number is easy to associate with the owner of the vehicle - and will not be discussed in any more detail here.

The other possibility, which is based on the *pre-paid* model, can be set up as follows. The road user deposits cash on his card - with digital cash - at fixed deposit points along the road, for example gas stations. The deposit points accept cash, which is then added to the value of the card as digital cash. Amounts are deducted from the card at so-called toll collection points. This is completely automatic with the aid of telecommunications. Each vehicle is equipped with what is called a transponder. The smart-card can be linked to the transponder, so that the smart-card can communicate with the toll collector (Stoelhorst, H.J. and Zandbergen, A. J., 1990). The card and the deposit points are made available by the toll collector. The above system is what is known as a closed system: the digital cash can only be spent at the toll booth. Appendix D describes an open system whereby the bank issues and accepts digital cash. In such a case, digital cash can be spent everywhere.

Digital cash consists of electronic documents that the toll collector signs with his digital signature. A road user may select the electronic documents himself. Each signed document represents a fixed value which allows the road user to pass a toll collection point. The road user sends a signed document to the toll collector at each toll collection point (see figures C.1 and C.2). The value of the signed document does not depend on the content of the document: it is important that the document be signed by the toll collector and no one else.

A variation of this system which offers less privacy protection is one in which the user is granted a single pseudo-identity by the toll collector. The road user goes by this pseudo-identity when communicating with the toll collector. However, the privacy of the road user is jeopardized as soon as it becomes possible to link the pseudo-identity with his real identity.

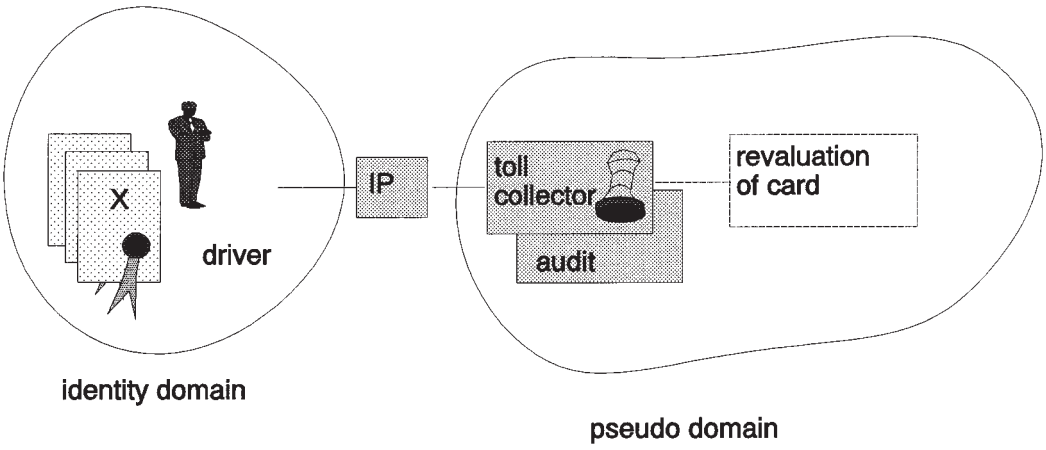

Figure C1: The toll collector signs with his digital signature the road user's electronic documents. Not the document's content but the toll collector's signature represents a value.

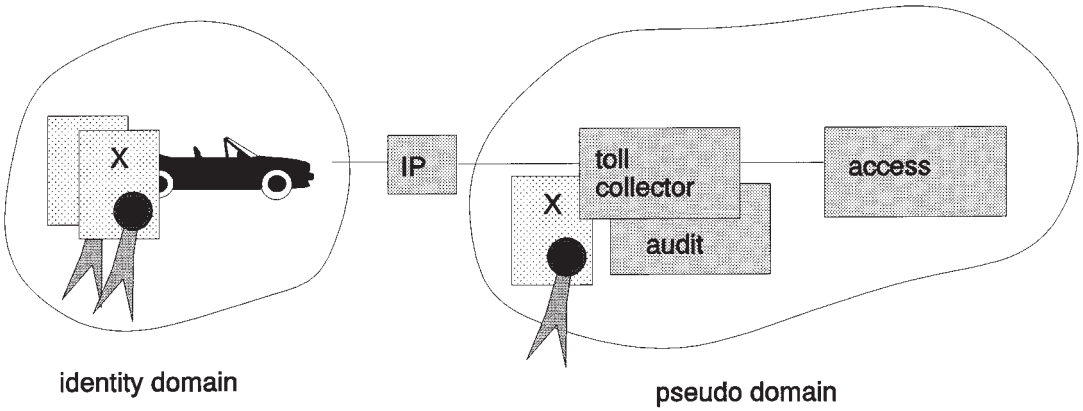

Figure C2: Each time a toll collection point is passed the road user sends a signed document to the toll collector. The toll collector's digital signature on the document is proof of its authenticity.

Summary and conclusion

A road-pricing system as outlined above would not allow the toll collector to trace the identity of the road user. In that case, the road user need not depend on the toll collector's good will when it comes to protection of his privacy.

Implementation of the system is a complex enterprise. A well-designed privacy information system can be completely undone if, for example, the transponder can be linked with the vehicle on which it is mounted. If the transponder has a unique identification number (e.g. a factory number stored in the equipment's hardware), then each transponder can be associated with the registration number of the vehicle on which it is mounted.

There are various possibilities for implementation when designing a road-pricing system. Designers must be aware of the locations in the system where the road user's identity can be tracked down. This part of the system should be minimized.

Appendix D: Digital Cash

Users can pay for articles purchased in a store in a number of ways: with cash, with a bank card, or with a credit card. The last two payment options involve use of data that can easily be linked with the user's identity. The bank statements the shopkeeper receives state highly identifying data, such as the account number and name of the user. If a user wants to remain anonymous, he is currently forced to use the first means of payment—cash.

System description

There are different ways to improve safeguarding user privacy when making payments. We will discuss three methods: procedural measures taken by the bank, pre-paid cash cards, and transferable credentials.

Procedural modifications by the bank

The only difference between this solution and customary payments with a bank card is that the shopkeeper does not receive the name and account number on bank statements. In this way, the shopkeeper cannot keep records on users and their spending patterns. The procedural measures at the bank consist of not stating the name/account number of the customer.

Pre-paid cards

It is possible to deposit cash onto a smart-card. The cards are issued by interested parties, such as a large chain of department stores or a bank. The cards are anonymous: no records contain information enabling the card to be linked with the user's identity. When payment is made, cash is deducted from the smart-card. These cards are also referred to as pre-paid cards. Pre-paid cards could also be used for road-pricing systems (see appendix C).

Cash or bank card money can be deposited on the card. Machines are required with which money can be deposited on the card. The service-provider has a machine to check whether the user has enough cash on his card. The service-provider can also use this machine to transfer cash from the user's card to his own card, till or account number. When a smart-card is used to deposit cash and make payments, the system must - if it is to protect the user's privacy - make it impossible to draw a link between the account number and the smart-card, which would be possible if the smart-card contained a unique serial or factory number and communicated this to the machine used to deposit cash on the smart-card.

The costs of copying a pre-paid card are not proportionate to the (limited) maximum amount that can be deposited onto it. The card is generally not secured against loss or theft. Someone who comes into possession of a lost or stolen card can use it without problems.

Telephone cards are an example of a pre-paid card. With such a card, telephone network services can be used, while the user remains anonymous. This card has a certain initial value. Each time a pay-telephone is used, the value is reduced. Cash can never, however, be added to this kind of card. If the card is stolen from or lost by the user, he loses the amount remaining on the card. From the perspective of privacy, it is better to use telephone cards with *smaller* amounts. A user can buy one telephone card worth twenty-five dollars and create one (big) pseudo-domain. Five telephone cards of five dollars each means that he creates five (small) pseudo-domains. Five different pseudo-domains affords the user more privacy than one large pseudo-domain.

Payment by credentials

A third way to *pay anonymously* is based on so-called transferable *credentials*. Here, blind digital signatures are used. The bank knows the user's identity, but with this method, the bank cannot find out where the user spends his money. Nor is the shopkeeper able to draw a link between the money and the user's identity.

Figure D.1 shows how a bank places a digital signature on an electronic document, say a bill, belonging to the user. This signature corresponds with a certain amount of cash: the bank uses a different signature for every fixed amount. This sum of money is deducted from the account as soon as the bank signs it. Figure D.2 indicates how the user can pay a shopkeeper under a pseudo-identity. He transfers the digital signature from his identity (ID) to his pseudo-identity (PID).

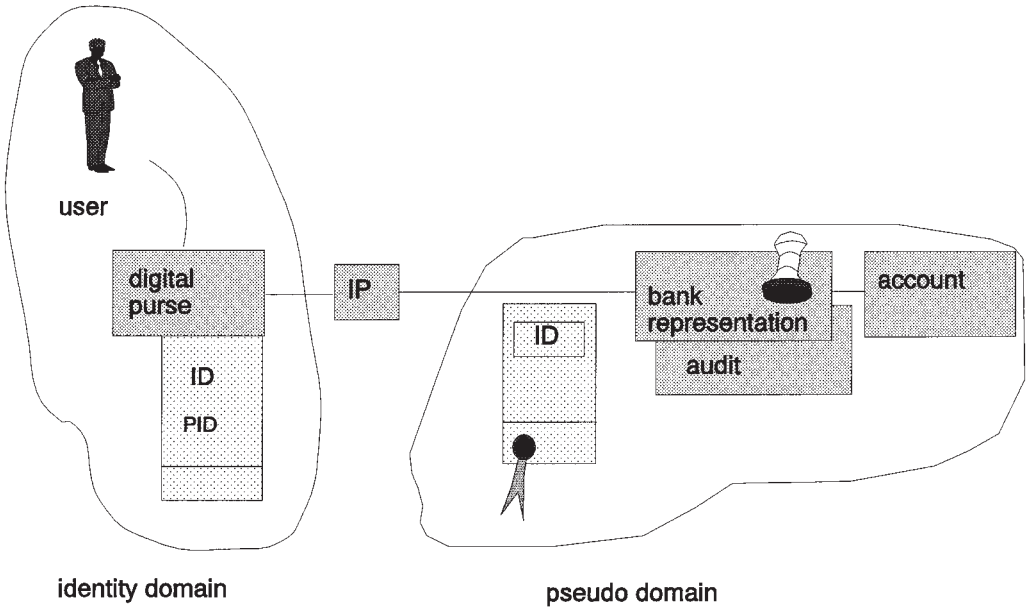

Figure D.1: The user produces a digital document with both his identity and a pseudo-identity on it. Before sending the document to the bank the user covers the pseudo-identity. The bank verifies the document, signs it and debits the user's account. After this transaction the user possesses a document representing a fixed value.

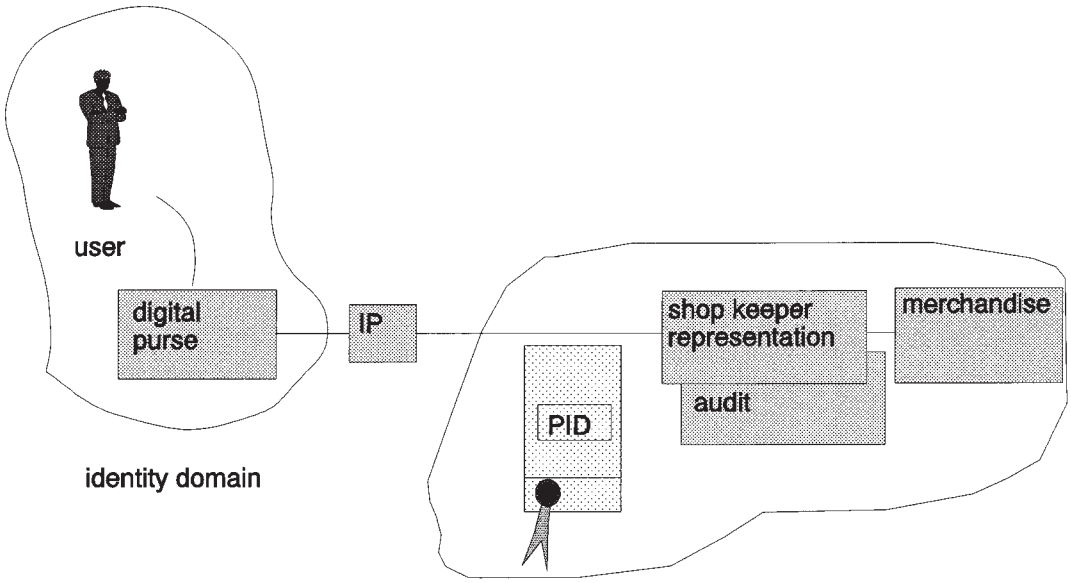

Figure D.2: The user enters a store. Before the signed document is handed to the storekeeper, the user covers his identity. The storekeeper can only read the pseudo-identity and the value. The bank's digital signature on the document is proof of its authenticity. The bank credits the storekeeper's account.

Conclusion

There are a number of ways to improve protection of the user's privacy when making payments. The options vary from simple procedural adaptations to entirely new systems. When procedural adaptations are made, the shopkeeper no longer receives the names of his customers on his bank statements. In this case, the user is dependent on the bank to protect his privacy. New systems make use of cryptographic techniques such as the digital signature which compel protection of the user's privacy.

Appendix E: Access control with biometric identification methods

System description

During the process of *access control* a service provider checks whether the user representation is authorized for each service provided. Access control takes place within the information system. As described in section 3.3.3, an internal representation can be used for this purpose without revealing the user's identity.

Such an alternative representation should be safe against misuse and practically feasible. New developments in biometric identification methods, based upon unique body characteristics of a person, fulfil these requirements, without the need to reveal a person's identity during the access control. Possible characteristics are fingerprints, iris patterns or retina pattern. The following example shows how the use of fingerprints has been realised for access control to e.g. buildings or personal computers.

Fingerprint identification

In order to authorize a person to access a certain object, building, or information system, a digital scan is made of the person's fingerprint. A number of particulars (so called minutiae) of the fingerprint pattern are measured, typically twenty, and their position is stored in a reference table. The data in this reference table form a unique identifier of a person; no other person will yield the same table. However, it is impossible to recreate the original fingerprint from the data in the table: the person's identity cannot be retrieved by comparing the data with a stored fingerprint image. Next, the table is encrypted and stored as a code on a chipcard.

If a person wishes to access the object, he presents the chipcard to a chipcard reader. Simultaneously a finger is presented to a fingerprint scanner, and a scan of the fingerprint is made. The results of the fingerprint-scan are measured and matched to the reference on the chipcard. If the two match, the person is given access.

A practical application is access control to personal computers in a hospital environment. A fingerprint scanner and a chipcard reader are built into the computer on the employee's desk. If a medical file is kept open without being accessed for a certain time, it will be automatically closed by the computer, and re-opened on presentation of the fingerprint of an authorized user. This solution is both safe and practical, since the fingerprint verification will only take a second or less, without unnecessarily interrupting activities.

This solution offers access control without revealing the person's identity. The transaction takes place within the pseudo-domain. The link between the identity of the person and the ownership of the chipcard is only present within a separate domain.

Discussion

Biometric identification methods potentially have a privacy-invading character, since the biometric data relate uniquely to an individual (Davies, S., 1998). However, as indicated above, through the way these methods are implemented in an information system, they can be transformed into a privacy enhancing technology.

Literature

Agre, P. and Rotenberg, M., (1997) *Technology and Privacy: The New Landscape.* MIT Press.

Bemelmans, T. M. A., (1987). *Bestuurlijke informatiesystemen en automatisering*. Stenfort Kroese.

Blarkom, G. van, (1998). Guaranteeing requirements of data-protection in a hospital information system with privacy-enhancing technology. In: *British Journal of Healthcare Computing & Information Management*, vol. 15, No. 4., May 1998, p. 30

Boe, E., (1994). Pseudo-identities in health registers? In: *The International Privacy Bulletin*, Volume 2, Number 3, July 1994.

Brands, S., (1993). Untraceable off-line cash in wallets with observers. Advances in cryptology. In: *CRYPTO '93*, August 1993, p. 302-318.

Brandt, J. e.a.. Anonymous and verifiable registration in databases, Advances in Cryptology. In: *EUROCRYPT 88*, p. 167-176.

Burkert, H. (1997). Privacy-enhancing Technologies: Typology, Critique, Vision. In: *Technology and Privacy, The New Landscape*, eds. Agre, P. and Rotenberg, M.. MIT Press,
p. 125-143.

Chaum, D., (1990). Showing credentials without identification transferring signatures between unconditionally unlinkable pseudonyms. Advances in cryptology. In: *AUSCRYPT '90*, January 1990 p. 246-264.

Chaum, D., (1987). Sicherheit ohne identifizierung. In: *Informatik-Spectrum*, (1987) 10: p. 262-277.

Chaum, D. and Pedersen T. P., (1994). In: *Wallet databases with observers*. 1994 p. 89-105.

Chaum, D. e.a., (1988). Untraceable electronic cash, Advances in Cryptology. In: *CRYPTO 1988*, p. 319-327.

Chaum, D., (1992) Achieving electronic privacy, a cryptographic invention known as a blind signature permits numbers to serve as electronic cash or to replace conventional identification. The author hopes it may return control of personal information to the individual. In: *Scientific American*, August 1992, p. 96-101.

Chaum, D., (1988) Dining cryptographers problem, the: unconditional sender and recipient untraceability. In: *Journal of cryptology*. 1988 nr. 1, p. 65-75.

Chaum, D., (1985). Security without identification: Transaction Systems to make big brother obsolete. In: *Communications of the ACM*, Vol. 28, no. 10, October 1985, p. 1020-1044

Cramer, Y., (1994). Chip-card als blackbox van de burger. In: *Technisch weekblad*, 21 september 1994, p. 15.

Cramer, R. J. F. and Pedersen, T. P., (1994). *Improved privacy in wallets with observers*. p. 329-343.

Dangerfield, W., e.a., (1993). Caller display and call return. In: *British Telecommunications Engineering, Vol. 12*, October 1993, p. 176-182.

Davies, S., (1998). Biometrics – A civil liberties and privacy perspective. In: *Information Security Technical Report*, Vol. 3. No. 1., 1998, p. 90-95.

Diffie, W. and Hellman, M. E., (1976). New Directions in Cryptography. In: *IEEE Transactions on Information Theory*, vol. 22, no. 6, November 1976, p. 644-654.

Galvin, J. M., (1989). Privacy without authentication. In: *Message Handling Systems and distributed applications*, 1989 p. 187-202.
Spreitzer, M. and Theimer, M. (1993). Providing Location information in a ubiquitous computing environment. In: *SIGOPS '93*, 12-1993, N.C., USA p. 270-283.

Girault, M., (1990). Three-pass identification protocol using coding theory, A (non-practical). Advances in cryptology. In: *AUSCRYPT '90*, january 1990 p. 265-272.

Goldschmidt, A. J. W. und Gal, L., (1991). Optimierte computergestützte zufallszahlengenerierung zur anonymisierung patientenbezorgener Informationen. In: *Software Kurier für Mediziner und Psychologen* 1991 nr. 4 p. 145-150.

Hayes, B. (1990). Anonymous one-time signatures and flexible untraceable electronic cash. Advances in cryptology. In: *AUSCRYPT '90*. January 1990 p. 294-305.

Hernon, P., (1994). Privacy Protection and the Increasing Vulnerability of the Public. In: *Government Information Quarterly*, Volume 11, number 3, 1994.

Kessel, W., (1998). *Datenschutzfreundliche Technologien, Arbeitskreis der Datenschutzbeauftragten des Bundes und der Länder*. Schwerin.

Mambo, M. e.a., (1992). Communication protocols with untraceability of sender and receiver. In: *Systems and computers in Japan*, Vol. 23, no. 9, 1992. p. 11-18.

Maurer, H. A. e.a., (1984). Videotex without "big brother". In: *Electronic publishing review*, Vol. 4, no. 3, 1984 p. 201-214.

Mjolsnes, S. Fr., (1991). Privacy, Cryptographic Pseudonyms, and the state of health. Advances in cryptology. In: *ASIACRYPT '91*. november 11-14, 1991, p. 493-494.

Pfitzmann, A. and Waidner, M., (1987). Networks without user observability. In: *Computer and security nr. 6*, 1987 p. 158-166.

PTT Telecom, (1993). *Euro-ISDN, User-networkaspect*.

Registratiekamer (1994). *Nummeridentificatie bij telefoonverkeer*, zaaknummer 93.A.012, 25

Rossum, H. van, (1994). *Beveiliging van persoonsregistraties*. Rijswijk: Registratiekamer.

Rotenberg, M., (1994). Privacy Protection. In: *Government Information Quarterly*, Volume 11, number 3, 1994.

Rothfeder, J., (1992). *Privacy for Sales: how computerization has made everyone's private life an open secret*. New York: Simon and Schuster.

Scarr, H. A., (1994). Privacy Protection and Data Dissemination at the Census Bureau. In: *Government Information Quarterly*, Volume 11, number 3, 1994.

Shizuya, H. e.a., (1990). Demonstrating possession without revealing factors and its application. Advances in cryptology. In: *AUSCRYPT '90*, january 1990 p. 273-293.

Solms, On. S. von and Naccache, D., (1992). Blind signatures and perfect crimes. In: *Computers & Security, 11 (1992)*. p. 581-583.

Stoelhorst, H. J. and Zandbergen, A.J., (1990). Development of a road pricing system in the Netherlands. In: *Traffic Engineering and Control*, February 1990 p. 66-71.

Trubow, G. B. Peeping Sam: Uncle is watching us. In: *Computer security journal*, Vol. IV, number 1, p. 15-20.

Tweede Kamer, vergaderjaar 1997-1998, 25816

Wright, T., (1993). *Smart cards*. Ontario, Canada: Information and Privacy Commissioner.

In de serie Achtergrondstudies en Verkenningen zijn reeds verschenen:

Artz, M.J.T. en Eijk, M.M.M. van, *Klant in het web, Privacywaarborgen voor internettoegang.* A&V-17, Registratiekamer, 2000. f 25.

Zeeuw, J. de. *Informatieverstrekking, Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving.* A&V-16, Registratiekamer, 2000. f 10.

Hes, R., Borking, J.J. en Hooghiemstra, T.F.M. *At face value. On biometrical identification and privacy.* A&V-15, Registratiekamer, 1999. f 10.

Artz, M.J.T. (1999) *Koning Klant. Het gebruik van klantgegevens voor marketingdoeleinden.* A&V-14, Registratiekamer, 1999. f 50.

Borking, J.J., e.a., *Intelligent software agents and privacy.* A&V-13, Registratiekamer 1999. f 40.

Hooghiemstra, T.F.M., *Privacy & Managed care.* A&V-12, Registratiekamer 1998. f 25.

Hes, R. en Borking, J. (editors) e.a. *Privacy-enhancing technologies: the path to anonimity.* revised edition. A&V-11, Registratiekamer 1998. f 25.

Almelo, L. van, e.a., *Gouden bergen van gegevens. Over datawarehousing, datamining en privacy.* A&V-10, Registratiekamer 1998. f 25.

Zandee, C., *Doelbewust volgen. Privacy-aspecten van cliëntvolgsystemen en andere vormen van gegevens-uitwisseling.* A&V-9, Registratiekamer 1998. f 25.

Zeeuw, J. de, *Informatiegaring door de fiscus. Privacybescherming bij derdenonderzoeken.* A&V-8, Registratiekamer 1998. f 25.

Hulsman, B.J.P. en P.C. Ippel, *Gegeven: de Genen. Morele en juridische aspecten van het gebruik van genetische gegevens.* A&V-7, Registratiekamer 1996.

Gardeniers, H.J.M., *Chipcards en privacy. Regels voor een nieuw kaartspel.* A&V-6, Registratiekamer 1995. f 25.

Rossum, H. van e.a., *Privacy-enhancing technologies: the path to anonymity,* volume I and II. A&V-5, Registratiekamer 1995. f 50 (uitverkocht).

Rommelse, A.F., *Zwarte lijsten. Belangen en effecten van waarschuwingssystemen.* A&V-4, Registratiekamer 1995. f 25.

Rommelse, A.F., *Ziekteverzuim en privacy. Controle door de werkgever en verplichtingen van de werknemer.* A&V-3, Registratiekamer 1995. f 25.

Casteren, J.P.M. van, *Bevolkingsgegevens: Wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden.* A&V-2, Registratiekamer 1995 (uitverkocht).

Rossum, H. van e.a., *Beveiliging van persoonsregistraties,* Registratiekamer 1994. f 25.

Deze publicaties kunt u bestellen bij de Registratiekamer, Postbus 93374, 2509 AJ Den Haag, telefoon 070-3811300, fax 070-3811301, onder vermelding van titel en auteur.

Registratiekamer

Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag
Telefoon 070 - 381 13 00
Fax 070 - 381 13 01
mail@registratiekamer.nl
www.registratiekamer.nl
August 2000