FIDIS

Future of Identity in the Information Society

Title:	"D14.2: Study on Privacy in Business Processes by Identity Management"
Author:	WP14
Editors:	Günter Müller, Sven Wohlgemuth (ALU-FR)
Reviewers:	Denis Royer (JWG), Jozef Vyskoc (VaF)
Identifier:	D14.2
Type:	[Deliverable]
Version:	1.0
Date:	Thursday, 15 March 2007
Status:	[Final]
Class:	[Public]
File:	fidis_wp14_d14.2-study_on_privacy_in_business_processes_by_identity_management-v1.0.doc

Summary

Privacy is not only a concern of customers. Service providers also fear privacy violations as a main hurdle for the acceptance of personalised services. Furthermore, the protection of privacy is an interest of service providers who take on customer relationship management activities of several service providers. They manage customers' profiles, e.g. in loyalty programs and e-health scenarios with electronic patient records, and offer the service of aggregation. If it is possible to link profiles of a customer without the need of such service providers, latter would not benefit from their aggregation service. Three case studies show privacy threats in business processes with personalised services.

The objective of this study is to identify privacy threats in business processes with personalised services, to suggest process models for modelling privacy-aware business processes and to derive security requirements for user-centric identity management in order to preserve privacy.

The scenarios and use cases presented in this study are recommended for non-technical readers, whereas the analysis of user-centric identity management protocols and approaches for identity management extensions are recommended for technical readers.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	30.10.2006	Initial release with first sketch of table of contents (Sven Wohlgemuth)
0.2	24.11.2006	Section "Personalised Profiles and the Need for 'Ambient Law'' (Mireille Hildebrandt) and section "Using Attributes as Access Rights in eGovernement (Jan Camenisch and Susan Hohenberger) added.
0.3	06.12.2006	Section "'Data Track' for Increasing Transparency for End Users" (Mike Bergmann, Simone Fischer-Hübner, Marit Hansen, Jan Möller and John Sören Pettersson) added.
0.4	07.12.2006	Section "Compliance in Enterprises – How can Trends in IT-Security be transferred to Data Protection?" (Martin Meints) added.
0.5	05.01.2007	Contribution of TUB (Richard Cissée) to outlook added.
0.6	20.01.2007	Sections "Personalised Services", "Communication Relationships in Business Processes", "Privacy Aspects", "Development of Privacy towards Data Protection", "Privacy and Security Threats" "Security Requirements for Privacy", "Business Processes and Identity Management", "Delegation of Rights by DREISAM" and "Conclusion and Outlook" (Sven Wohlgemuth) added.
0.7	16.02.2007	Section "Privacy-aware Business Process Design by an Enterprise Privacy Architecture" (Günter Karjoth), sections to case study *loyalty program*, executive summary and introduction added (Sven Wohlgemuth)
0.8	19.02.2007	Case study "Intelligent Software Agents" added (Ammar Alkassar)
0.9	26.02.2007	Study for internal review (Sven Wohlgemuth)
1.0	15.03.2007	Study revised according to internal review (Sven Wohlgemuth)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary)	Sven Wohlgemuth (ALU-FR)
2 (Introduction)	Sven Wohlgemuth (ALU-FR)
3 (Information Chains in Personalised Business Processes)	Ammar Alkassar (SIRRIX) and Sven Wohlgemuth (ALU-FR)
4 (Privacy and Data Protection in Business Processes)	Ammar Alkassar (SIRRIX), Mireille Hildebrandt (VUB) and Sven Wohlgemuth (ALU-FR)
5 (Privacy-aware Business Process Design and Identity Management)	Jan Camenisch (IBM), Susan Hohenberger (IBM), Günter Karjoth (IBM), Martin Meints (ICPP) and Sven Wohlgemuth (ALU-FR)
6 (Approaches for Identity Management Extensions for Business Processes)	Mike Bergmann (TUD), Simone Fischer-Hübner (KU), Marit Hansen (ICPP), Jan Möller (ICPP), John Sören Pettersson (KU) and Sven Wohlgemuth (ALU-FR)
7 (Conclusion and Outlook)	Richard Cissée (TUB), Sven Wohlgemuth (ALU-FR)

Table of Contents

1 Executive Summary

Privacy is not only a concern of customers. Service providers also fear privacy violations as a main hurdle for the acceptance of personalised services (Sackmann and Strüker, 2005). Furthermore, the protection of privacy is an interest of service providers who take on customer relationship management activities of several service providers. They manage customers' profiles, e.g. in loyalty programs and e-health scenarios with electronic patient records, and offer the service of aggregation. If it is possible to link profiles of a customer without the need of such service providers, latter would not benefit from their aggregation service.

The **target audience** of this report is twofold: chapter two to four are more for non-technical readers whereas chapter five and six are refer to technical reader, since among others identity management protocols are examined in detail with respect to the scenarios of this study.

The **objective of this study** is to identify privacy threats in business processes with personalised services, to suggest process models for modelling privacy-aware business processes and to derive security requirements for user-centric identity management in order to preserve privacy.

Figure 1.1 shows the **approach of this study**. Based on privacy as informational self-determination, privacy threats are identified in business processes by the reference scenario. This reference scenario is used as an orientation for the authors of this study. Undesired profiling is in particular investigated by case studies. The investigation of profiling differs in unconscious collection of customers' data by service providers and in externally stored customers' profiles and delegation of access on some of these profiles by customers. To get a survey on the use of collected customers' data in business processes, to derive access rights on these data from data protection legislations and agreements and to suggest a method for evaluating privacy-aware business processes, two process models are described. From the technical viewpoint, representatives of user-centric identity management protocols based on credentials are applied on single-stage and in particular on multi-stage business processes in order to show their suitability for preventing undesired profiling. Security requirements for user-centric identity management in multi-stage business processes are the result of this investigation. As countermeasures for (a) undesired profiling with delegation of rights and (b) unconscious collection of customers' data, the extensions (a) *DREISAM* for an unlinkable delegation of rights and (b) *Data Track* for tracking disclosure of personal data by customers are introduced as extensions for identity management.

The **results of this study** differ in unconscious collection of customers' data and in the prevention of profiling if customers delegate rights to service providers in order to get access on some profiles for a specific purpose.

Unconscious collection of customers' data and their aggregation with individualised profiles lead to a threat to personal autonomy because customers are not aware of the way their preferences are manipulated. Customers should have the opportunity to access on unconscious collected and aggregated profiles and to adapt their profiles in order to make these profiles transparent to them. Since data protection legislations lack of effectiveness in the sense that service provider implements the minimal part so that they are not sanctioned and in the lack of control of each service provider, customers should have an instrument for counter profiling so that they are aware of an unconscious data collection. The *Data Track* mechanism is an

approach for such a transparency instrument; however, it supports solely conscious data collections up to now.

Concerning delegation of profiles, current user-centric identity management systems do not achieve data economy. If current identity management systems are used, a service provider acting on behalf of a customer gets access to customer's complete identity. The challenge is to control the disclosure of personal data to personalised services and at the same time to prevent undesired profiling about the customer. The *DREISAM* protocols achieve an unlinkable delegation and revocation of access rights. Proxies do not get identifying data of customers by a delegation, if identifying data are not needed for the purpose of their service. Thus, the knowledge of service providers managing customers' profiles is kept confidential and they are able to benefit by an aggregation of their profiles under restriction of customers' consent. Therefore, *DREISAM* implements a mechanism for usage control with regard to customers' data.

Further work investigates on the verification of service providers whether they have processed customers' data according to the negotiated arrangement between service provider and customers as well as according to the given data protection legislation. The objective is to get evidences concerning the use of customers' profiles. In order to technically re-trace the information flow of disclosed customers' data, the study "D14.3: Study on the Suitability of Trusted Computing to support Privacy in Business Processes" of the FIDIS Work Package 14 "Privacy in Business Processes" investigates on trusted computing as a platform to support the enforcement of privacy policies by service providers.

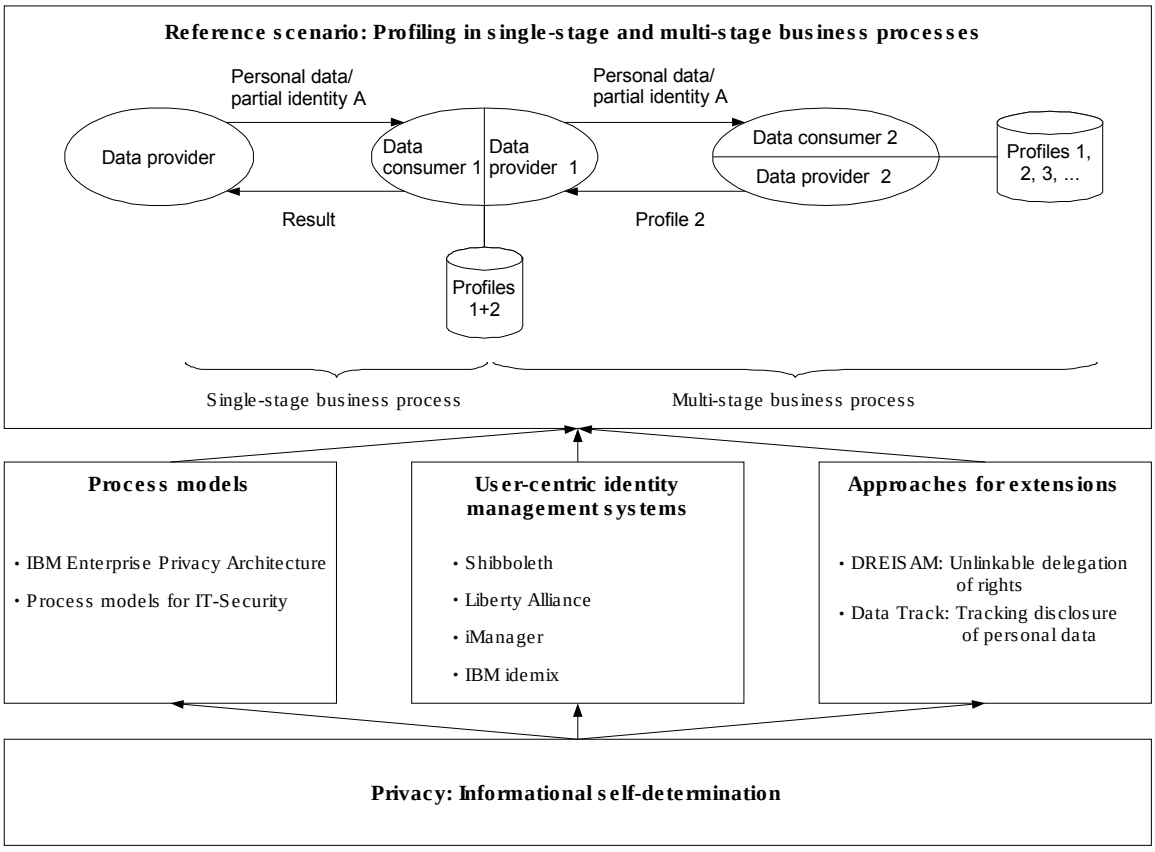

Figure 1.1 Approach of FIDIS deliverable D14.2.

2 Introduction

2.1 Scope

The objective of this study is to identify privacy threats in business processes with personalised services and to present technical approaches for usage control and transparency mechanisms. These approaches extend user-centric identity management. This study investigates on privacy threats in single-stage and multi-stage business processes in particular with regard to profiling of customers by service providers. In case of an unconscious data collection in ambient intelligence environments, e.g. in sensor networks, the need of implementing data legislation in devices is motivated. The aim is to achieve transparency to customer with regard to the unconscious data collection. Multi-stage business processes realise business models where profiles of customers are externally managed by a special service provider. Examples are loyalty programs and e-health applications with electronic patient records. Process models for modelling privacy-aware business processes are presented. While they assume trust of customers to service providers, current user-centric identity management systems are investigated in detail according to their suitability as a security mechanism for privacy in single-stage and in particular in multi-stage business processes.

In contrast to the FIDIS study on a "structured overview on prototypes and concepts of identity management systems" (deliverable D 3.1[1]), the identity management protocols are hereby analysed in detail. As an extension for user-centric identity management, the usage control mechanism *DREISAM* and the transparency mechanism 'Data Track' are presented afterwards. This study concludes with an outlook on further work concerning the verification of a compliant use of disclosed personal data with regard to data protection legislation and the negotiated agreements between customer and service providers.

2.2 Structure and Content

This study is organised in four parts:

- **Part 1: Privacy threats in business processes with personalised services**
- **Part 2: Privacy-aware business process design and identity management**
- **Part 3: Approaches for identity management extensions for business processes**
- **Part 4: Conclusion and outlook**

Part one introduces two scenarios for business processes with personalised services: single-stage business processes and multi-stage business processes with service providers acting on behalf of their customers. The aim of **part two** is to derive security requirements for identity management which preserve customer's privacy with regard to his informational self-determination, i.e. a customer is able to decide on the disclosure and use of his personal data. Furthermore, part two investigates on process models for inventing privacy in business processes and on the current security mechanism for private data: identity management. Current user-centric identity management systems classified concerning the trust model are

[1] Available at www.fidis.net

considered and applied on both types of business processes. **Part three** presents two approaches for identity management which partially fills this gap by a credential-based usage control mechanism and a transparency instrument for customers in order to retrace their data disclosure and profiles at service providers. **Part four** concludes this document and gives an outlook to further work in order to verify the trustworthiness of the participating service providers and certification authorities.

3 Information Chains in Personalised Business Processes

Personalised services and business processes are adapted to customer's personal data and attributes to address them among others according to their interests and to offer them individual discounts. This chapter investigates on information chains regarding customer's personal data and on the two types of scenarios with personalised services according to the communication relationship of customers with service providers. If personalised services are combined in a business process, some service providers act on behalf of customers. In this case, a customer does not use directly each service in a business process but uses it in a *1:n:m* communication relationship via another service provider which is called his proxy. For this purpose, a customer delegates some personal data or attributes to his proxy so that this proxy is able to use subordinate services according to customer's interests. Automation of business processes is realised by coupling autonomous services, e.g. web services, to establish an information system for the purpose of a business process.

Section 3.1 introduces personalised services by their goals and support of information systems. Section 3.2 classifies business processes by their communication relationships of customers who either directly or indirectly interact with service providers. Concerning personal data, a direct communication relationship focus on disclosing personal data where an indirect communication relationship focus on the use of disclosed personal data. Section 3.3 shows that privacy violations are a hurdle for service providers to offer personalise services. Section 3.4 presents a case study as an example for personalised services with direct and indirect communication relationships: loyalty programs. Section 3.5 presents a case study where autonomous software programs, intelligent software agents, act on behalf of a customer in order to arrange a travel. Section 3.6 concludes this chapter.

3.1 Personalised Services

The basis for the realisation of personalised services is the collection and usage of personal customer data. According to the *Electronic Commerce Enquête IV (ECE IV)* (Sackmann and Strüker, 2005) survey with regard to the German market, almost two-thirds of the enterprises participating (65.2 %) stated that they use customer data. 51.7 % of these enterprises already use the collected data for the analysis of the payment behaviour of the customers and a further 4.7 % plan to use customer data for this purpose within the next two years. In second place is the analysis of the purchasing history of their customers, which is conducted by 45.6 % of the respondent enterprises with customer data. It even stands in first position with 7.0 % for the planned usage of customer in the next two years. Only 17.6 % use the data of their customers for the social-demographic analysis according age, gender or standard of education of their customers. The surfing behaviour of their customers is, on the other hand, only evaluated by 6.3 % of the participating enterprises. Finally, with the use of customer data the participating service providers pursue the goals of personalised address of their customers (57.0 %), an individualisation of purchasing discussions (53.8 %) and an adaptation of their products or services to their customers (47.4 %). Over half the enterprises that already use customer data plan to expand their current activities.

If one considers the differences between the various enterprise size ranges, then it appears that personal data of their customers is primarily collected and used by major enterprises irrespective of the concrete form of the data. Hence, 53.4 % of 146 major enterprises, 44.0 % of 141 medium-sized enterprises, 38.9% of 131 small enterprises use the purchasing of their

end customers. Most of the enterprises are thereby engaged in the branches of the manufacturing trade (44.2 %) and the credit and insurance business (42.1 %).

3.1.1 Personalisation through Customer-Oriented Business Processes

An utilisation of personal data of customers and customer-oriented business processes involved is summarised under the term of Customer Relationship Management (CRM). With the employment of CRM systems an enterprise aims at (Bange and Schinzer, 2005)

- a minimisation of investment costs for customer search,
- a maximisation of the sale of private production capacities and services, and
- possible long-term customer loyalty with the enterprise.

CRM is thereby no one-show conducted measure, but a continuously repeated process consisting of analysis and awareness gaining phases, strategy development and planning, interaction with the customer as well as refinement and adaptation. A service provider thus aims at the optimisation of customer profitability of the whole life cycle of a customer starting from customer identification through to improvement of customer value and continued existence of customers. A customer is thereby individually addressed (personalisation) and integrated into the production process (mass customisation) (Banke and Schinzer, 2005).

3.1.2 Architecture of the General CRM System

CRM systems are used to support customer orientation, whereby a general CRM system is comprised of the three subsystems of operative, collaborative and analytical CRM and adapts the business processes of a service provider to the individual attributes of a customer. Figure 3.1 shows the architecture of a general CRM system.

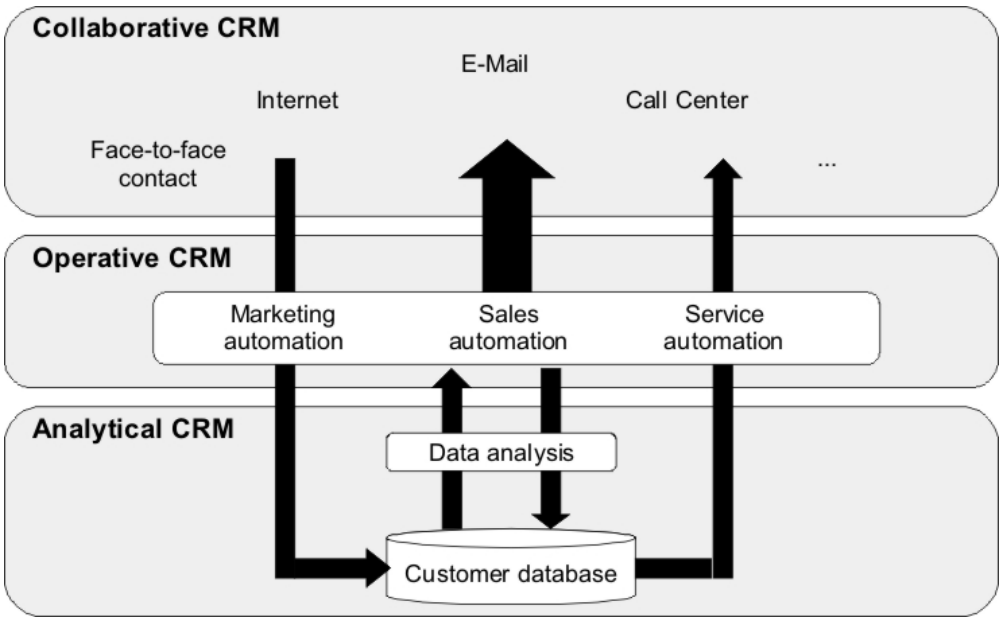

Figure 3.1 Architecture of the general CRM system (Banke and Schinzer, 2005).

The **collaborative CRM subsystem** constitutes the interface of the service provider to his customers. The various communication channels are shown adaptively to the customer's end device. The **operative CRM subsystem** adapts the business processes to the individual customers by having access to the data collected about the customers and controlling the information flow of the customer data for the business processes concerned. It contains functions for automating sales, marketing activities and for customer service. The task of the **analytical CRM subsystem** is the analysis of the collected customer data with regard to a customer-oriented business processes. The central element thereby is the customer database which is used by a service provider to manage customers' data, which he has received by a data collection with the operative CRM subsystem or from external data sources. The aim of an analysis of the customer data is to recognise the needs, potentials and risks with prospective and established customers and there from derive measures for a personalised customer address.

With the development of monolithic and (in the course of time) proprietary IT systems towards distributed and dynamical IT systems, an automated and dynamical realisation of service processes is becoming possible which supports an intercompany networking (Huhns and Singh, 2005). Hagel and Brown (Hagel and Brown, 2001) underline the differences between both types of IT systems and the employment possibilities of an IT system in accordance with the SOA. It is thus difficult to adapt business processes dynamically to the market changes according to new functionality and restructuring with former IT systems. These IT systems in fact predetermine business processes. Enterprises can develop their IT system according to their business processes with the flexibility and an open standardised architecture of an IT systems according to service-oriented architecture (SOA), concentrate on their core competencies, offer them as a service for further service providers and integrate into their own IT system the required functionality depending on the requirements of a business process during its life-span.

3.2 Communication Relationships in Business Processes

The interaction of a customer with a service provider takes place, amongst others, via so-called process portals. A process portal pools all services and information of a service provider for a certain process, whereby own services as well as services of further cooperating service providers are included (Schmid, Bach and Österle, 2000). The portal-operating service provider also adopts the role of a process specialist in addition to the role of a service integrator – i.e. he guides his customers through the process.

The interaction between a customer and integrated services takes place in a direct and, in the case of a multi-stage business process with a chain of services, in an indirect communication relationship. A direct communication relationship is a *1:n* relationship of a customer with n service providers, whereby an indirect communication relationship is a *1:n:m* relationship from a *1:n* relationship between a customer and *n* service providers and a subsequent *n:m* relationship between n service providers who communicate directly with the customer and m service providers who provide a service for the customer but are not in direct contact with him.

3.2.1 Single-stage Business Processes: Collecting Customer's Data

Single-stage service processes are characterised by the customer knowing each service provider involved in the process and that these provide the required service without further

support. The customer conducts the process whereby each service is invoked by him. If further services are required for a process, the customer initiates the next service required in the process and passes the result of the preceding service on to it. No interaction for executing the process takes place between the services involved in the business process.

As the services are personalised services, the customer discloses personal data at the service providers' request. In Figure 3.2, the data is called *pers. data* and *partial identity A* or *partial identity B.* The governor of the data or partial identities is named the data provider, as he regulates the access to this data. The recipients of the data, who then also process it for the respective service, are called data consumers. Through the disclosure of personal data or partial identities to service providers, a profile of the customer is generated with them. The profiles are shown in Figure 3.2 with *profile 1* and *profile 2*. It is assumed that the profiles do not necessarily contain the same data about the customer.

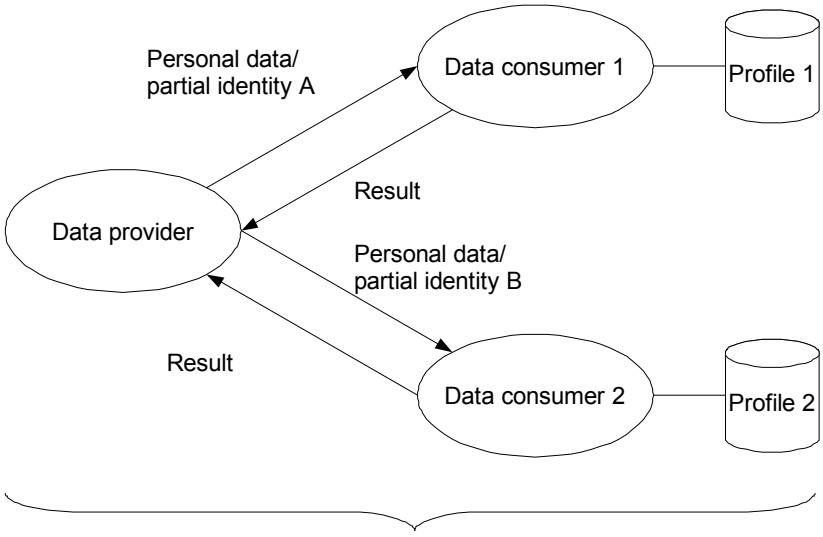

Figure 3.2 Single-stage business process and the creation of customer profiles.

3.2.2 Multi-stage Business Processes: Using Customer's Data

Multi-stage business processes are characterised by a chain of series-connected service providers within a process. A resultant intercompany networking thereby pursues effectivity and efficiency goals. In the German market 45.7 % of the enterprises interviewed within the scope of ECE IV are networked with IT systems of other enterprises via the Internet. 52.5 % of the enterprises therewith pursue efficiency goals, such as reduction of costs, and effectivity goals, such as the integration of external services into their own range of services of offered. 63.4 % of the enterprises interviewed currently plan to extend their activities. With 70.6 %, the credit and insurance industry presents the overall largest share of enterprises that are intercompany networked (Sackmann and Strüker, 2005).

A multi-stage business process is also initiated by a customer with requesting a known service provider. The latter requires certain data of the customer for providing his service. This is summarised in Figure 3.3 in the *partial identity A.* The *data consumer 1* processes this data. For the customer, this has the advantage that he does not necessarily have to know the

process, i.e. he does not require any knowledge about the entirety of the services required and their progression with the related conditions and commencing and terminating events. For further execution of the process, the *data consumer 1* however requires further personal data of the customer, which is called *partial identity B*. At this point, a multi-stage business process differs from a single-stage business process. The customer's profile which is generated with *service provider 1* no longer just contains the data of the *partial identity A*, but also of the *partial identity B*, which are intended for the *service provider 2*. The merging of profiles with *service provider 1* is shown in Figure 3.3 with *profiles 1+2*.

Furthermore, the *service provider 1* changes his role where the subsequent *service provider 2* is concerned. He now appears a proxy and thereby as *data provider 1*. The *service provider 1* must be able to use the *partial identity A* for the use of the services of the *data provider 2*. This *data provider 2* returns *profile 2* of the given customer to *data provider 1*, who is in this case in the role of *data consumer 1*. Since *data provider 2* collects profiles of customers, this service provider takes up the role of a data consumer, here *data consumer 2*, too. A change of role is not thereby fixed for a certain service provider but depends on the process.

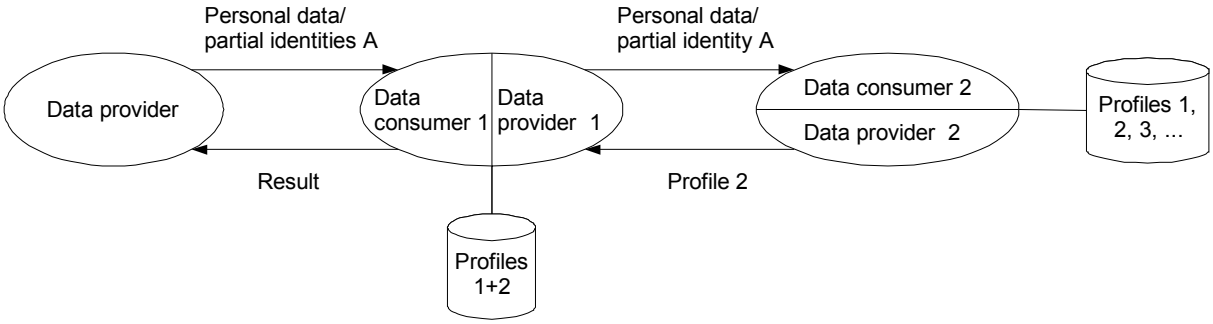

Figure 3.3 Multi-stage business process and delegation of profiles.

3.3 Hurdles for the Acceptance of Personalised Services

According to the *ECE IV* survey, German market enterprises regard the protection of privacy and the protection of their customers' data as two significant hurdles for the supply of personalised services. According to the most significant hurdle, the intricate and cost intensive integration of personalised services into existing processes and existing organisation (87.9 %), 84.1 % of the participating enterprises expect a negative customer reaction owing to a violation of their privacy, 84.2 % doubt the compliance with the data protection laws and 81.9 % expect a lower customer acceptance (Sackmann and Strüker, 2005). Better services, individualisation of services and convenience for the customer are therefore faced with the dangers of manipulation of identity, profiling, identity theft and undesirable delegation of personal data (Kruelle, Swatman, Rebne and Hampe, 2002).

3.4 Case Study: Loyalty Program

The use of customer data in business processes is shown by an exemplary case study: *Loyalty program*. Loyalty programs aim to commit customers to specific companies. These companies delegate their customer relationship management to a loyalty program provider. The loyalty program provider manages the profiles about customers of this loyalty program, offers personalised services, sends them advertisements, and gives customers premium points,

whenever they buy goods or services at companies which take part in this loyalty program. By these premium points, customers are allowed to get discounts on goods or pay other goods or services with these points. Each customer gets an own loyalty card with a unique card number for authentication. A customer can have one or more loyalty card for different programs. Loyalty cards are issued by merchants or the loyalty program provider. Latter is assumed for this case study. A loyalty card is technically realised by a credential.

3.4.1 Business Process: Collecting Customer's Data

Each time a customer uses his loyalty card while buying goods or services, the corresponding loyalty program partner forwards the services or goods which have been sold, their price, the discount, and the date of the selling together with the customer's loyalty card number. Loyalty program partners are data consumers concerning collection of customer's data and data providers regarding the delegation of customers' profiles to the loyalty program provider. It is assumed that loyalty program partners store the profiles about their customers. In the following, a loyalty program partner is considered as a merchant. Figure 3.4 shows this scenario. The card number is given by *Card ID* and customer's data concerning one loyalty partner are summarised by *selling data*. An example for a loyalty program is the German PAYBACK loyalty program. This loyalty program consists of 52 companies of different branches, e.g. retail, medicine, and insurances[2].

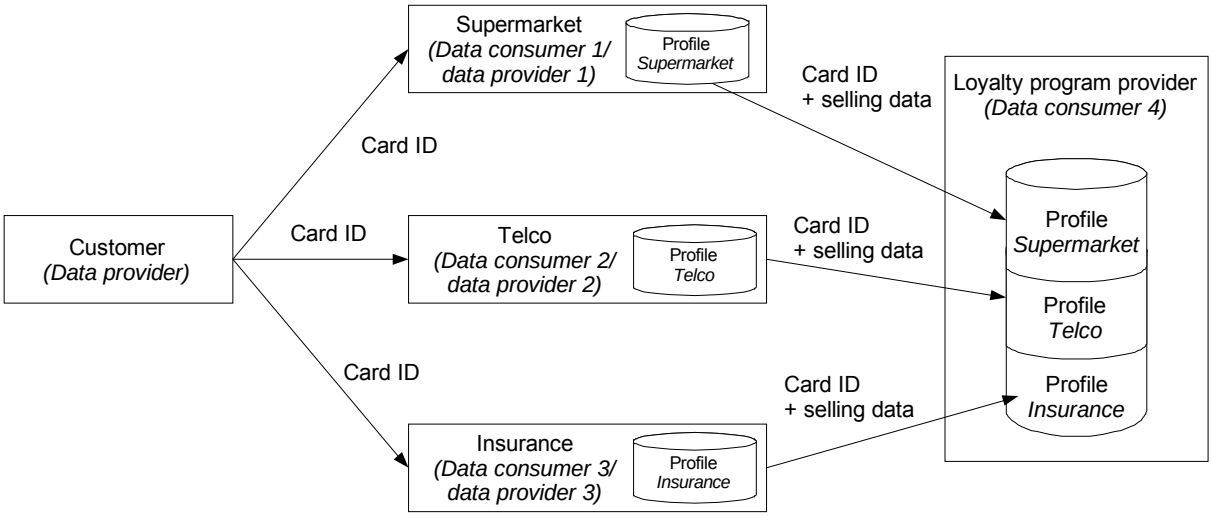

Figure 3.4 Collecting customer's data.

3.4.2 Business Process: Using Customer's Data

The extension of the previous scenario is that a customer wants to show some of his properties to a merchant in order to get special benefit for a personalised service, e.g. to show that he does not smoke in order to get discount on a private health insurance. The customer enhances his reputation at the insurance company by showing his buying history at the supermarket in order to prove that he has not bought tobaccos. So, the customer specifies this purpose of using one of his profiles by delegating an access right to the insurance company to

[2] http://www.payback.de, last accessed at February 2007

access his profile *supermarket* at the loyalty program provider. It is assumed that the loyalty program provider discloses customers' profiles only with their authorisation. In Figure 3.5, the insurance company (data consumer 3) gets this access right on customer's profile with respect to his buying history.

Since the loyalty program provider does not disclose customers' profiles, the insurance company asks the given customer for allowing access on customer's buying history of his *supermarket* profile. The customer delegates the *read* authorisation concerning this request for a one-show use to the insurance company in step two. This insurance company acts in step three as a proxy for the customer, since the customer does not retrieve this data himself at the loyalty program provider. If this authorisation is valid, the loyalty program provider grants the desired access and denies it otherwise. So, the loyalty program provider has changed his role from a data consumer (*data consumer 4*) to a data provider (*data provider 4*). Privacy threats for customers concerning these two business processes are identifies in section 4.4

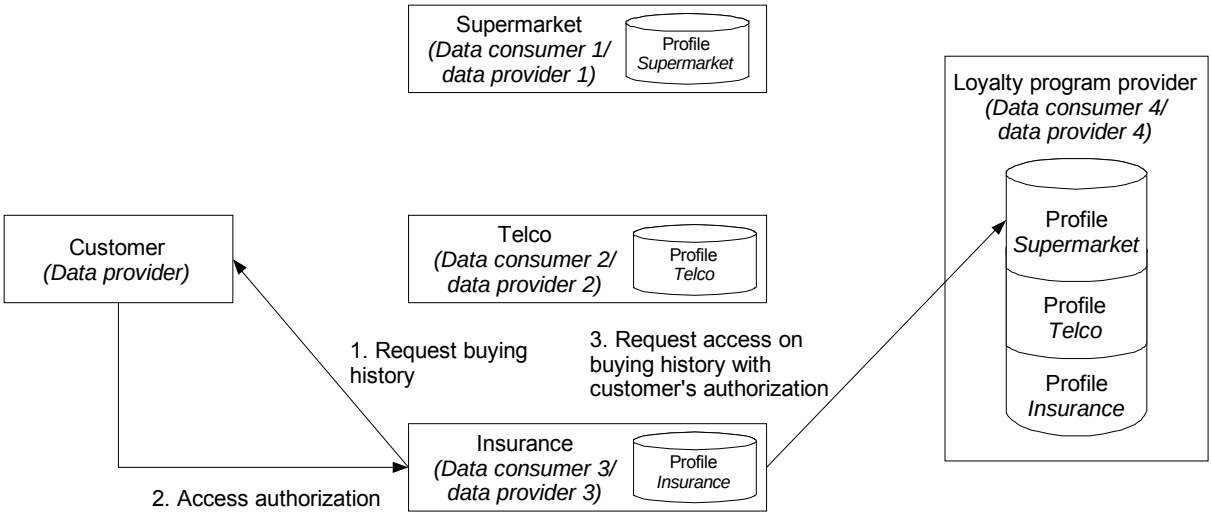

Figure 3.5 Delegation of access rights with regard to customer's supermarket profile.

3.5 Case Study: Intelligent Software-Agents

A Software-Agent is defined as a piece of software that is acting on behalf of its user. Its objective is to take over tasks and to finish them without a direct interaction or permanent supervision by the user. Originally developed for telecommunication services, e.g., collecting information for the user, today, "Intelligent" Software-Agents (ISA) are designed to complete tasks on behalf of the user.

Agents for that purpose contain a profile of their users, including personal data. The data in this profile are the basis for the actions the agent performs: searching for information, matching the information with the profile and performing transactions on the behalf of the user.

Two examples may illustrate the application scenarios of Intelligent Software Agents:

For Instance, imagine an ISA, participating on the user's behalf in an auction system, say E-Bay. Another example is a travel agent service that is implemented by an Intelligent Software

Agent. There, the ISA not only researches for the best travel opportunities (probably most convenient and economic), but also do the binding reservations and bookings (cf. Figure 3.6).

Thus and at first glance, ISA appear to hold out great promise for automating routine duties and even conducting high level transactions. However, looking beyond the functional requirements, it becomes clear that ISA could present a significant threat to privacy relating to the privacy of personal information in their possession and under their control. Accordingly, it is highly desirable that their development and use reflect European privacy standards (i.e. EU Directive on Privacy and Electronic Commerce 2002/58/EC) in order to protect the personal information of their users.

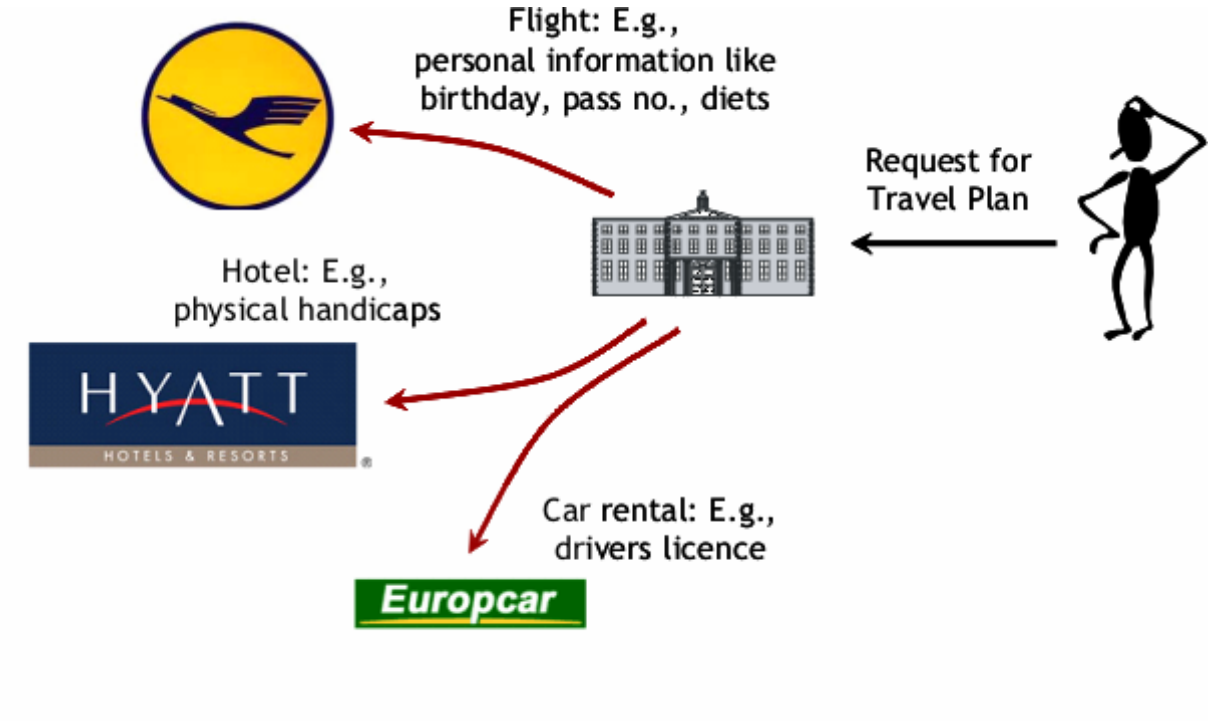

Figure 3.6 Travel agents need a lot of sensitive financial and personal information to process their task.[3]

The whole raison-d´être of the ISAs is to act on the user's behalf and function as the user's trusted personal servant, serving one's needs and managing one's organizational activities.

Thus, their powers are constrained by a number of factors: the degree of software complexity (the rules they can fulfil), the number of services with which they can interact, and, most importantly, the amount of personal information that they possess about the user.

Because agents could be requested to perform any number of tasks ranging from downloading the daily newspaper to purchasing concert tickets for a favourite singer, the agent is required to know many of information about the user.

[3] Company logos are registered trademarks.

In order to function properly, an ISA must also have the following characteristics:

- Mobility to act within open communications networks
- Deliberative behaviour or an ability to take an action based on a set of criteria
- The ability to act autonomously, co-operatively, and to learn.

In section 4.5 we will have a look on the privacy threats with respect to ISA.

3.6 Conclusion

Business processes are becoming increasingly oriented to the interests of a customer. In addition to the collection of personal data, its delegation and usage by service providers in place of the customer as far as further service providers are concerned is necessary. An example for business processes with delegation is an application making use of customers' profiles hosted externally by a data service provider. Profiles are thereby desired, so that the principle of data economy does not fit anymore with regard to privacy. The use of personal data leads, however, to privacy problems that are considered to be an important acceptance factor. The following chapter focuses on privacy of customers and security interests of service provider in business processes with personalised services.

4 Privacy and Data Protection in Business Processes

The aim of this section is to define the term of privacy for this work and to identify the threats that exist for a customer with single and multi-stage business processes. Section 4.1 lead to an understanding of privacy for business processes. As sensor networks are used for business processes, e.g. by the METRO Future Store, interactions between customers and service providers get unconsented by customers. Personal data is collected without notification. Customers are not aware of the content of their profiles which are created by service providers. Section 4.2 focuses on unconsented profiling and introduces the need for 'Ambient Law' as an instrument for customers in order to retrace the collection and use of personal data. Section 4.3 describes privacy threats in general if personal data are disclosed and delegated in business processes. Section 4.4 picks up this kind of authorisation and presents in the case study *loyalty program* profiling as a privacy threat if personal data as access rights are delegated to service providers. Section 4.5 shows privacy threats if software agents get customers' data act on behalf of them. Section 4.6 summarises the analysis of this chapter.

4.1 Privacy Aspects

Privacy applies to various aspects of an individual. The *Privacy and Human Rights 2005* report of the *Electronic Privacy Information Center* and of *Privacy International* (EPIC, 2006) divides the term of privacy into the following four areas:

- **Location-related privacy**: This aspect concerns intrusions into the individual's privacy within specific environments, e.g. his own living area, place of work and publicity and sets limits to their intrusion. Examples of such intrusions are video surveillance and identity establishment by means of personal identity cards.
- **Body privacy:** The aspect of body privacy concerns the protection of the physical person against undesirable intervention, e.g. gene analysis, medication tests and the taking of blood samples.
- **Private communication relationships:** This aspect concerns a secure and private communication of any kind, whether it is by letter post, telephone or email.
- **Private data:** This aspect concerns the development and enforcement of rules for the collection and processing of personal data. These rules are summarised under data protection.

The following work focuses on private data.

The term *privacy* has a varying significance depending on the view of the individual and activities with data about him (Solove, 2006a) and in various environments in which the individual moves. In addition, it has changed during the course of time due to grand circumstances (cf. the introduction of a legal force for the avengement of violation towards the individual through the *Justice of the Peace Act 1361* (Moir, 1969) and the speech of the English parliamentarian and later Prime Minister William Pitt in 1765 about the privacy of the individual in his house or dwelling place (Pitt, 1765), in 1948 the admittance of the protection of privacy into the human rights through the United Nations (United Nations, 1948) and above all since 1890 through the technical development (cf. the undesirable acceptance of photos of persons and their unconsented publication (Waren and Brandeis, 1890)). Particularly the technical development through to electronic data processing, starting

from a central processing in computer centres through to a distributed processing in client-server architectures and their networking via the Internet up to ubiquitous computing has changed the term of privacy by way of informational self-determination (Westin, 1967; German Federal Constitution Court, 1983) through to present-day data protection laws and directives (European Commission, 1995; German Federal Government, 2001; European Commission, 2002), which ultimately provide protection principles for the processing of personal data (Roßnagel, 2005).

William Pitt regarded an individual's affairs in his own home as privacy affairs which had to be protected from the king, i.e. the force of the state and to which he should have no access: "*The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; storm may enter; the rain may enter — but the King of England cannot enter; all his force dares not cross the threshold of the ruined tenement!*" (Pitt, 1765).

Samuel D. Warren and Louis D. Brandeis, a later federal judge of the United States of America saw a privacy intrusion due to the technical developments, such as, amongst others, instant photos and their commercial use in daily newspapers which happens without the consent of the person photographed however and therefore with possible accompanying impairment of their reputation. For the term of privacy, they take up the expression of "*right to be let alone"* and specify the protection against an undesirable intrusion into the privacy of the individual (Warren and Brandeis, 1890).

The General Assembly of the United Nations sees a human right in the protection of privacy and lays this out in its declaration (United Nations, 1948) as an ideal of the member states to be striven for and guaranteed. In addition to the private dwelling, privacy also applies to the communication of the individual, to his honour and his reputation. The spread of privacy is therefore extended to the relationships of the individual with other persons and to his appearance.

4.1.1 Privacy as Informational Self-determination

With the start of electronic data processing for societal purposes, e.g. for a census, and economic purposes, e.g. end customer governing of a business venture, a more simple combination of data, i.e. a profile generation of the individual and a more rapid analysis of the profiles generated compared to a manual one through the computing power available becomes possible. Accompanying this is the low control of the individual over the collection, processing, storage and transmission of the data collected (Henderson, 1999). There is now the danger of the inappropriate collection of personal data, its abuse, e.g. for advertising purposes and for identity theft. With an identity theft, another person acts with the identity of another person but without the consent of the person concerned. Furthermore, there is the danger that decisions such as on creditworthiness and entry into a state are met exclusively on the basis of the collected data.

In view of the spread of electronic data processing, the information flow of personal data was included in the term of privacy by Alan Westin: "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"* (Westin, 1967). The protection of personal data for its collection and use was specified in 1983 under the concept of *informational self-determination* for the first time by the German Federal Constitutional Court in the so-called

"census judgment" and established as a basic right: "*Under the terms of modern data processing, the protection of the individual against unlimited collection, storage, use and transmission of his personal data is covered by the general personal rights of Art.2 paragraph. 1 Basic Constitutional Law in connection with Art.1 paragraph. 1 Basic Constitutional Law. The basic right insofar guarantees the power of the individual to basically determine for himself about the disclosure and usage of his personal data*" (German Federal Constitution Court, 1983). This judgment however limits the right to informational self-determination, if there is a vast general interest for the limitation.

4.1.2 Privacy by Data Protection

The named technical development threats through to electronic data processing with regard to informational self-determination led to the German and European Data Privacy Laws (cf. (Roßnagel, 2005)). The general basic principles of the Data Privacy Law that are transcribed in the European Data Privacy Directive 95/46/EC (European Commission, 1995) which was extended for a general electronic communication through the European Data Privacy Directive 2002/58/EC (European Commission, 2002), and in the German Federal Data Protection Act (German Federal Government, 2001), are:

- Transparency of data processing through briefing and notification of the person concerned,
- Necessity of the data collected for a certain purpose,
- Restriction of data processing to a certain purpose,
- Correction rights of the person concerned on the required data and the processing phases,
- Data avoidance and economy,
- Data protection through technology, and
- Implementation control through a data protection representative.

The minimal principles for privacy protection found in the named Data Privacy Directive of the European Union originate from the *Fair Information Practices*. These principles were first published in the *United States Departments for Health Education and Welfare* (HEW) report and were incorporated in the *US Privacy Act of 1974* (cf. (Smith, 1993)). The five principles of *Fair Information Practices* are:

- **Collection limitation:** No secret system for collecting personal data may exist.
- **Disclosure:** A person must have the possibility to look at the profile generated on him and its use.
- **Secondary Usage:** It must be possible for a person to prevent the use of his profile for other purposes if he does not agree with the intended use.
- **Record correction:** It must be possible for a person to correct or add to a profile with personal data generated about him.
- **Security:** An organisation that generates, maintains, uses or spreads personal data must, on the one hand, ensure that this data is used for the intended purpose and, on the other hand, take precautionary measures to avoid an abuse of the data.

These five principles were accepted by the *Organization for Economic Cooperation and Development (OECD)* and standardised in the form of eight principles for the protection of privacy in cross-frontier data exchange through the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 1980). This involves the following principles:

- **Collection Limitation Principle:** The range of the profile generated should suit its purpose of use. Data collection should take place with legal means and with the knowledge or consent of the person involved.
- **Data Quality Principle:** The data collected should be related to the purpose and be necessary. Furthermore, it should be correct, complete and up-to-date.
- **Purpose Specification Principle:** The purpose of the collection of personal data should be specified at the point in time of collection at the latest. If the purpose of use changes, this change should also be specified. In addition, further use of the data collected for fulfilling this purpose or equivalent purposes should be restricted.[4]
- **Use Limitation Principle:** Personal data may not be published, made available or in any way used for purposes other than those specified. An exception to this is if the owner of this data has agreed to it or in the case of a judicial authority.
- **Security Safeguards Principle:** Personal data should be protected by suitable security measures from unintentional loss and unauthorised access, obliteration, use, modification and publication.
- **Openness Principle:** There should be a general policy of openness that gives information about the developments, practices and guidelines of the organisation with relation to the personal data collected by it. Means should be available to the individual for determining the existence and motive for the data collection, the main purposes of use of the collected data and the data protection representation of this organisation.
- **Individual Participation Principle:** An individual should have the right
    - to learn from a data protection representative of an organisation whether and, as the case may be, which personal data has been collected about him by the organisation,
    - to be informed about the data collected within a suitable time, possibly for a not too exorbitant fee, in a suitable way and in a form comprehensible to him,
    - to receive a reason if one of the above two requests have been rejected and be able to contest such a rejection, and
    - to challenge a collection of data and, if the challenge has been successful, arrange the erasure, correction, completion or modification of the profile.

[4] New purposes of use should not be introduced haphazardly and be compatible with the purpose already specified. If collected data is no longer required for the specified purpose, it should be erased or anonymous, providing that this is possible.

- **Accountability Principle:** A data protection representative should guarantee the observance of the means with which these principles are executed.

4.2 Personalised Profiles and the Need for 'Ambient Law'

If we are to believe Philips (Aarts and Marzano 2003) and the European Commission (ISTAG 2001) we will be living in ambient intelligent environments sooner rather than later. This means that our offline environment will be enhanced with sensor-technologies and RFID systems, interconnected via online databases that allow re-iterant profiling and real time adaptation of the environment to our inferred preferences (ITU 2005).

In such an ambient intelligent environment data can be aggregated and processed by means of knowledge discovery in data bases (KDD) to detect patterns of behaviour of clients (Custers, 2004). KDD cannot be equated with queries is a database, as these depend on *prior* classification (Zarsky, 2002). Instead data mining techniques like KDD for instance *produce* clusters of *previously unknown* sets or association rules not thought of by the data analyst. This implicates that such data mining or profiling generates new types of knowledge, which can than be applied and tested on new instances until the patterns are considered stable enough to apply to (potential) clients.

The result of this type of processing of personal and other data recorded and aggregated from an ambient intelligent environment will be a series of dynamic group profiles (Bohn and Coroama, 2005). If, for instance, behavioural biometric profiling becomes a reliable tool for assessing emotional states or intentional stances,[5] this could in fact allow highly personalised profiles, constructed from intelligent combinations of individual profiles and a diversity of group profiles applicable to a particular individual. Such combinations will thus enable custom-made autonomically applied personalised services.

4.2.1 Effects of Intelligent Personalisation

The application of such combined profiles to an individual person may have a significant impact on the risks and opportunities that are attributed to this person (Zarsky, 2005). Real time monitoring and targeted servicing could allow refined segmentation of the market, providing previously unknown possibilities for price-discrimination. This regards buying and selling of consumer products like foodstuffs, cars or even real estate; services like hotel and catering industry, insurance, credits, but – if delivered to government agencies - could also be used for purposes of taxation, fraud detection and crime prevention.

A second effect may be that as service providers are capable of anticipating a change in our preferences this not only allows them to cater to new preferences, but also give them an opportunity to influence our behaviour if these changes are not profitable. For instance, if I am on the verge of quitting the smoking of cigarettes, advanced profiling technologies may be aware of this and alert tobacco industry. I may be confronted with extra banners for smoking at specific times, calculated to have optimal impact and/or I may be provided with free

[5] On behavioural biometric profiling see Yannopoulos, Andronikou and Varvarigou 2008 (FIDIS deliverable 7.5). In the Netherlands speech recognition systems are being used in Groningen to detect aggressive outburst in public spaces in order to prevent violent escalation. Bruno van Wayenburg, Relalarm vangt boze stemmen op, *NRC Handelsblad* 14th November 2006, p. 6 Wetenschap. The institute developing the technology is online at http://www.soundintel.com/index-en.html (last visited on 20 November 2006).

samples when ordering groceries from a supermarket. Such targeted 'servicing' seems a threat to our personal autonomy, mainly because we are not aware of the way our preferences are being manipulated (Zarsky, 2002). Being autonomous implies having the possibility to reflect on alternative choices of action, which is complicated if our environment influences our choices as it were 'behind our back'.

4.2.2 Data Minimisation and the Vision of AmI

The problem with personalisation based on refined combinations of automated group and individual profiles is twofold:

1. a person will not often be aware of the fact that a profile is constructed and applied;
2. she generally has no access to profiles that may be applied.

Present data protection legislation is focused on the protection of *personal data* and has little to offer in terms of making *profiles* transparent. This is for instance the case because profiles will mostly be inferred from data coming from other people, thus not qualifying as personal data in terms of art. 2 (a) of the directive (Zarsky, 2002).

One could of course claim that data minimisation will reduce the total amount of data and thus reduce the possibility of inferring adequate profiles. However, to generate adequate personalised services, especially in the case of Ambient Intelligence (AmI), as many data must be collected and processed as possible. Holding back data would most probably make the environment less intelligent, because the process of KDD or pattern recognition will be based on incomplete data. This could imply that while data mining techniques like privacy preserving data mining (PPDM) (Meints, 2008) may solve some of the privacy problems, the use of PPDM will also reduce the effectiveness of real time monitoring and real time adaptation of networked environments.

4.2.3 Data Maximisation and Personal Autonomy

If it is the case that an intelligent environment thrives on data maximisation – using profiling techniques to discriminate between noise and information, then we should consider the consequences of the realisation of the vision of Ambient Intelligence. The crucial issue here is control and this can be explained in terms of two requirements from the perspective of clients in a business process:

- access to the autonomically generated profiles that may be applied to them[6] and
- the possibility for (potential) clients to actively adapt their own profiles

This is the only way to effectively empower clients to act in ways that prevent undesired categorisation, and to anticipate the potential consequences of legitimate categorisation.[7] Personal autonomy does not mean that one is capable of complete isolation or opacity; it

[6] This would fit what has been called the principle of minimum information asymmetry (Jiang, 2002).

[7] About profiling as a type of categorisation see (Schauer, 2003; Hildebrandt, 2008).

rather demands that one has the instruments to counter profile one's environment, including the behaviours of intelligent machines or software programs.[8]

4.2.4 The Need for a Vision of 'Ambient Law'

To regain control in an AmI world, clients will need the right to have access to automated profiles that may be applied to them[9] and the right to actively adapt their own profiles.[10] But new legal regulations in the sense of enacted written law will not suffice. The problem with data protection legislation, as with all administrative law, is a lack of effectiveness. If there is no incentive for service providers to comply with the law they will only implement it in as far as they expect to be checked and sanctioned. The costs for governments to institutionalise adequate monitoring of service providers are simply too high and at this moment in time the transaction costs for clients to find out which profiles may be relevant, let alone to actively adapt them to their conscious preferences are way beyond measure.

In the course of the FIDIS cooperation within the work package on profiling we have come to the conclusion that to achieve an effective legal regulation of the access to profiles (including the possibility to contest them), these regulations must be articulated in the technological design of AmI devices. The *vision* of AmI thus requires a *vision* of Ambient Law. At present work package 7 on profiling is preparing the ground for a report on such 'Ambient Law', to be finalised in the middle of 2007. For a start such ambient law would for instance require:

1. technological embodiment of mandatory data protection legislation, effectively ruling out non compliance by service providers
2. technological embodiment of transparency, for instance requiring a user's proxy that is able to detect the types of profiles that may be applied and that warns the user if this may be disadvantageous
3. technological embodiment of machine to machine (M2M) communication to negotiate with the service provider about the level of anonymity and unlinkability
4. technological embodiment of machine to machine (M2M) communication to negotiate about the application of profiles predefined by the (potential) client; such negotiations could concern the terms of the contracts made between service provider and client, for instance the price, the exchange of data etc.

---

[8] A provisional definition of counter profiling could be: 'the use of KDD techniques to enable pattern recognition regarding the behaviours of human and nonhuman agents that use KDD to recognise and act upon a persons habits, life style, desires and preferences'. In FIDIS deliverable 7.9 and 7.13 the idea of counterprofiling as a transparency tool will be further developed.

[9] Art. 15 of the directive (D46/95 EC) grants a right not to be subject to automated individual decisions, based on the automatic processing of data. It is not clear to what extent this right can be waived by not exercising it and the right is restricted in paragraph (2) of art. 15. Art. 12 does grant a right of access to the logic of the automatic processing of any data concerning the person, 'at least' in the case of decisions described in art. 15. cf. (Bygrave, 2001).

[10] Art. 12 of D95/46 EC grants a right of access to data relating to a person and a right to rectify erase or block data that were processed in violation of the directive. This does not amount to a right to deliberate participation in the construction of profiles (erasing automatically generated profiles that one does not agree with or changing the parameters to what one claims to be one's preferences).

Having access to the types of profiles that may be applied will reduce the risk of falling victim to illegitimate price (or other) discrimination and should counter attempts to manipulate behaviour without awareness of the client.

4.2.5 Conclusion: The Design of Technologically Embodied Law

An AmI environment will facilitate business processed leading to profits for service providers and benefits for their clients. Protection of personal data is not the only issue that is stake if the vision of AmI is realised; protection against illegitimate or undesirable application of automatically generated profiles is needed. To achieve such protection legal provisions need to be embodied in technological devices other than the script (Lévy, 1990) in order to establish a renewed balance between the power of those that profile and those that are being profiled.

4.3 Privacy and Security Threats

As can be seen from the historical development of the term *privacy*, there is no standard definition for it. *Privacy* is in fact developing due to the technical developments and the associated possibilities of the partially oblivious formation of profiles, e.g. via surveillance cameras and goods marked with RFID tags (Sackmann, Strüker and Accorsi, 2006), and the processing of the profiles formed hardly comprehensible to the persons concern (Roßnagel, 2005). For this reason, privacy is defined for this work indirectly via the possibilities of information gain about the customer and the use of profiles formed for providers of personalised services. The interpretations of privacy above only assume a threat during an activity if the customer has not agreed to it. It is therefore assumed in the following that there is no agreement of the customer concerned on hand and that it involves activities of service providers and thus threats to his privacy.

A conception classification on the basis of the possible damages was made in 1960 by William Prosser (Prosser, 1960) and 2006 by Daniel J. Solove (Solove, 2006a). Prosser extended and structured the damage events of Warren and Brandeis (Warren and Brandeis, 1890). He defines the four damage categories of intrusion, public disclosure, false light and appropriation. However, Prosser refers exclusively to civil law offences. Moreover, technology on ubiquitous data processing for spontaneous networking of computers of varying computing capacity, network connection and size has advanced since 1960. Solove considers this technical development in his conception (Solove, 2006a). Based on his classification of the potentially damage-producing activities, the threats for a customer in single and multi-stage business processes are derived in the following.

4.3.1 Use of Personal Data

The activities of a service provider with the personal data of his customers apply in the CRM area to (1) collection, (2) processing, (3) storage and (4) transmission of customer data and to the (5) breaking into the customer's system and theft of his data. The threats relate exclusively to data that is confidential for the customers concerned and should therefore only be known to him and a circle of participants chosen by him. If this circle is extended without his consent, then his privacy is violated. The participants in the privacy model based on (Solove, 2006b) are a customer, service providers, and observer of the communication relationships between customer and service providers.

The threats to private communication relations are based on a communication of a third party not participating in the communication that could both actively modify the communication and with it the data of the customer as well as pass himself off as customer and by that be a man-in-the-middle. As passive observer, the threats of a profile creation about the customer by means of his communication with service providers emanate from him. Figure 4.1 shows this first part of the attacker model.

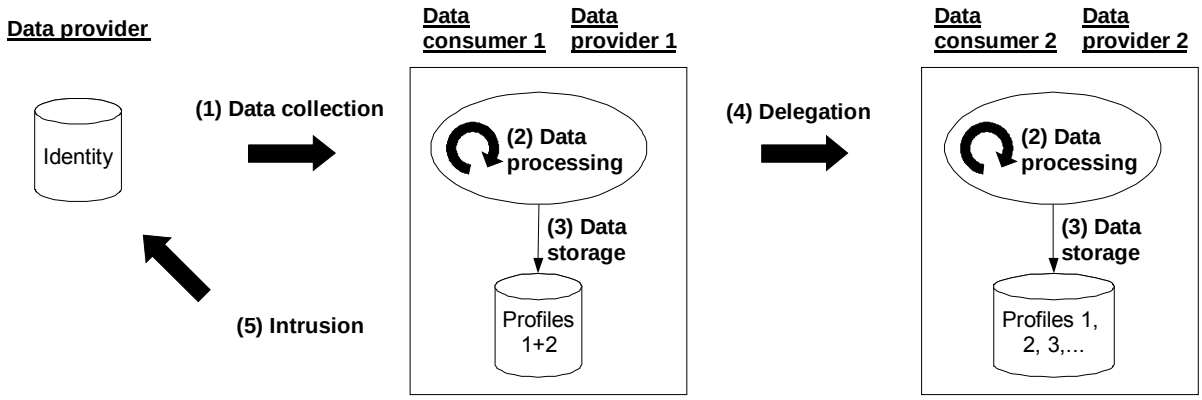

Figure 4.1 Activities with relation to the personal data of a customer.

The second part applies to the threats to personal data. Figure 4.2 highlights the participants concerned from whom the threats emanate and the related activities. An end device of the customer is assumed for the communication with the service provider. This can be any computer with connection to a computer network, e.g. a personal digital assistant (PDA) with radio networking possibilities. A web browser is used as application for the interaction. The entire personal data of the customer concerned is pooled under his identity and governed either on his end device or with a trustworthy party.

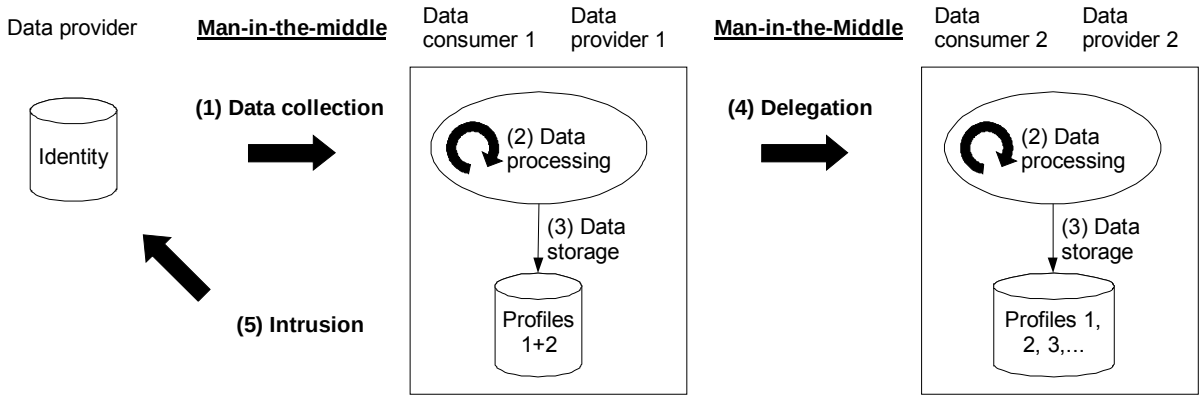

Figure 4.2 Activities of a man-in-the-middle with relation to personal data of a customer.

4.3.2 Collection of Personal Data

The collection of personal data takes place both consciously and obliviously to the customer. In the case of a conscious collection of data, a service provider requests certain personal data of a customer. Examples are delivery address or credit payment details. Web forms serve, amongst others, for the input. A customer can then decide whether he wishes to release the requested data to this service provider. In the case of oblivious data collection as happens, for example, with surveillance through video cameras in businesses (Ball, Lyon, Wood, Norris and Raab, 2006), with the collection of the IP address of the customer's computer or end device (Zugenmaier, 2003; Müller and Wohlgemuth, 2005) and with the readout of RFID-tagged goods (Strüker and Sackmann, 2004; Langheinrich, 2005), that the customer has purchased, he does not have this opportunity to decide.

While the customer recognises the purpose for a conscious collection of data by means of the associated service, an oblivious collection of data poses a threat to his privacy. This is due to the customer on the one hand not knowing what data about him is collected and, on the other, does not know the recipient and purpose of use of this data. The threats come from an observer of the communication of the end customer and service provider with whom he is communicating.

The collection of clearly identifying data about the customer presents a further threat to privacy. Examples of clearly identifying data are his personal identity card number, social insurance number and the MAC address of his end device. A linking of his transactions is possible by means of this data which, in turn, leads to a connection of individual profiles on the customer.

A profile about the customer ultimately emerges that contains data from a data collection agreed to and an oblivious one. As the oblivious part is unknown to the customer, the situation of an asymmetric information distribution arises between the customer and the service provider. Price discrimination is a negative consequence for the customer, i.e. a product is offered to him at a higher price compared to other customers. Pricing therefore leads to his disadvantage and cannot be comprehended by him (Eifert, 2004).

4.3.3 Processing of Collected Personal Data

The processing of collected personal data exclusively concerns the use of the data collected. The storage and transmission of personal data is also separately examined in the following sections. Data about a customer from possibly various sources is pooled in a business process during processing. Such a profile formation can have advantages for the customer. Hence, Amazon.com uses customer data to recommend individual products to them on the basis of their previous purchasing history. Through the use of so-called *recommender systems*, the effort in searching similar products is reduced (Lam, Frankowksi and Riedl, 2006). However, such profiles can become disadvantageous for the customer if they are used for decisions, e.g. for the approval of a funding, and in doing so the data in the profiles is not up-to-date. This can lead to the desired service being declined or offered on poorer terms on the basis of outdated customer data, although it would be offered for up-to-date customer data and, as the case may be, on better terms (Solove, 2006b).

A further threat to a customer's privacy in business processes is the use of collected data for purposes other than intended. On the one hand, this is the aggregation of individual profiles about the customer. If it takes place without his consent, the service providers involved gain

access to customer data to which they should not really be able. In consequence, service providers can derive additional interests, ways of behaviour, his creditworthiness and, in the case of a mobile customer, also his movement profiles (Müller and Wohlgemuth, 2005), about which they should not gain any knowledge. The confidentiality of individual profiles is no longer given and his privacy is violated.

From the main property of multi-stage business processes, the delegation of personal data to a service provider to use where further service providers are concerned, results in an abuse of this data as a further threat. A use for purposes other than intended and therefore an abuse of this data is the case when it is used by a service provider for a purpose other than the one to which the customer gave his consent for collection or delegation. In this case, there is a breach of trust by the acting service provider. The consequences of an abuse depend on its type of application. For instance, a case of abuse is if the data is used for advertising which the customer considers to be a nuisance and if financial damage is incurred for the customer through the data abuse. An example is the abuse of credit card data, if it is used for unauthorised payments by his proxy. Since the proxy appears under a partial identity of the customer, the last type of abuse is tantamount to an identity theft.

4.3.4 Storage of Collected Personal Data

It can be generally assumed that the purpose of a data collection and processing stretches over a certain period of time. The data collected is then stored by the service provider. The service provider has access to this data within this period of time. Since the purpose-related access takes place with the customer's consent, his privacy is maintained. Storage presents a threat to his privacy when the data storage temporally exceeds the customer's consent and an obsolete profile of the customer is used for the service of the service provider.

If the purpose of the data collection is fulfilled, e.g. a service provider has completed his task as proxy and rendered his service, the transaction between a customer and proxy is terminated. The customer's consent to the data processing also expires with this termination, i.e. the respective service provider is no longer authorised to access this data. However, if it is still possible for him to access his data, then this situation presents a threat to privacy. A potential attack is the appearance of a service provider with the stored (partial) identity of the customer after the course of a transaction. It is also to be considered here, however, that data can be stored beyond the purpose for the collective good. This is how things stand with the retention of telecommunication data to be used for tracing criminal offences (European Commission, 2006).

4.3.5 Delegation of Collected Personal Data

In the scenario of multi-stage business processes, personal data is disclosed by a service provider acting as proxy to further service providers. This, in turn, takes place with the consent of the respective customer. With his consent, the customer has specified the amount of subjects who can have access to and use this data. Delegation poses a threat, however, as a proxy can also disclose the data to other service providers. The amount of access and usage subjects specified by the customer is then relinquished. This proxy has consequently contravened the interests of the customer and violated his privacy. Such a disclosure constitutes a loss of confidentiality of this data and of the trust of the customer in his proxy. The linking of profiles and identification of the customer can, among others, be negative consequences, unless his data does not implicitly identify him.

The European Privacy Policy stipulates the notification of the person concerned with the first-time transmission of his data (European Commission, 1995). The German Teleservices Data Protection Act (TDDSG) allows the transmission of customer data for the purpose of market research which must however be anonymous (German Federal Government, 1997).

4.3.6 Intrusion into the Customer's System

In the scenarios of single and multi-stage business processes, it is assumed that a customer governs his data either on his personal end device or externally with a trustworthy party. He or the trustworthy party thereby governs the access to his data. A threat lies in faulty and damaged software, such as viruses or Trojan horses, whose aim is access to and a delegation of this data.

4.3.7 Threats to the Security of Service Providers

Privacy, however, does not only concern the interests of the individual and, in this case, the customer. The European Data Privacy Directive 95/46/EG, as German Federal Data Protection Act and the "census judgment" of the Federal Constitutional Court explicitly enable exceptions if the general interest predominantly necessitates this. This applies, amongst others, in the case of state prosecution (European Commission, 1995). There is then a case of fraud through the customer or his proxy.

In the first case, a customer denies a service received. The second case arises in multi-stage processes and assumes a fraudulent proxy. The threat occurs if this proxy deals in the customer's name and denies the transaction made with regard to the service providers concerned and the customer. In order that a prosecution is possible, the service provided must be able to be clearly related to the customer or his proxy. This complies with the protection goal of accountability of the multilateral security concept (Rannenberg, Pfitzmann and Müller, 1999).

4.4 Case Study: Privacy Threats in a Loyalty Program

The attacker model focuses on privacy threats of customers which are at the same time security threats of the loyalty program provider. Merchants are seen as attackers on privacy. Their aim is to link customers' transactions and thereby to create a profile by virtually combining their single, merchant-dependent profiles. Figure 4.3 shows the privacy problem when using a loyalty card for getting premium points. Figure 4.4 shows the privacy problem when delegating an access right on a specific customer's profile.

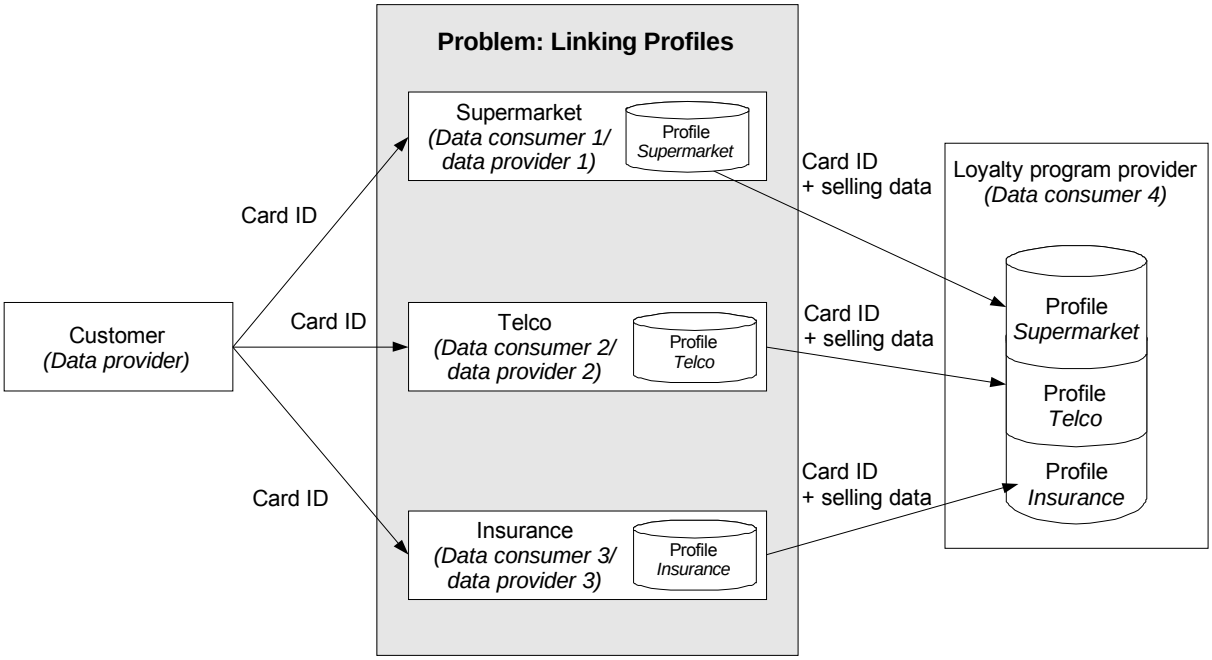

Figure 4.3 Linking customer's profiles by merchants when buying goods or services with a loyalty card.

Merchants are able to link their profiles by the unique card number (*Card ID*) of customer's loyalty card. It follows that they know what this customer has bought at the supermarket, the pharmacy, and the insurance company.

Privacy as informational self-determination is violated: the customer is not able to determine the disclosure of personal data. By linking profiles, customer's data are disclosed to other merchants and used for other purposes than those of the collection, since his profiles are now used by other merchants, too. Additionally, linking profiles is not an interest of the loyalty program provider. The collection of these profiles at his database empowers the loyalty program provider to analyze customers' profiles and to offer queries for marketing purposes. If the merchants are able to link their profiles without the loyalty program provider, the collection of profiles is worthless for the loyalty program provider. A merchant would not pose such a query at the loyalty program provider anymore.

If a customer delegates an access right on his profile to a merchant, he has two options for delegation:

- The customer issues a delegation credential for the merchant, e.g. a X.509 Proxy Certificate (Von Welch, Foster, Kesselmann, Mulmo, Pearlman, Tuecke, Gawor, Medder and Siebenlist, 2004).
- A CA issues a delegation credential for the merchant on behalf of the customer, e.g. a SPKI certificate (Ellison, Frantz, Lampson, Rivest, Thomas and Ylonen, 1999) or a Kerberos proxiable ticket granting ticket (Kohl and Neuman, 1993).

In both cases, transactions of a customer are linkable by every merchant and, in the second case, also by the CA. In the first case, the digital signature of the customer for his delegation credential makes him traceable. In the second case, the identifier of a customer is fixed in a

credential and obvious for every participating service provider. Figure 4.4 shows the profiling possibility for the second case, if Kerberos is applied.

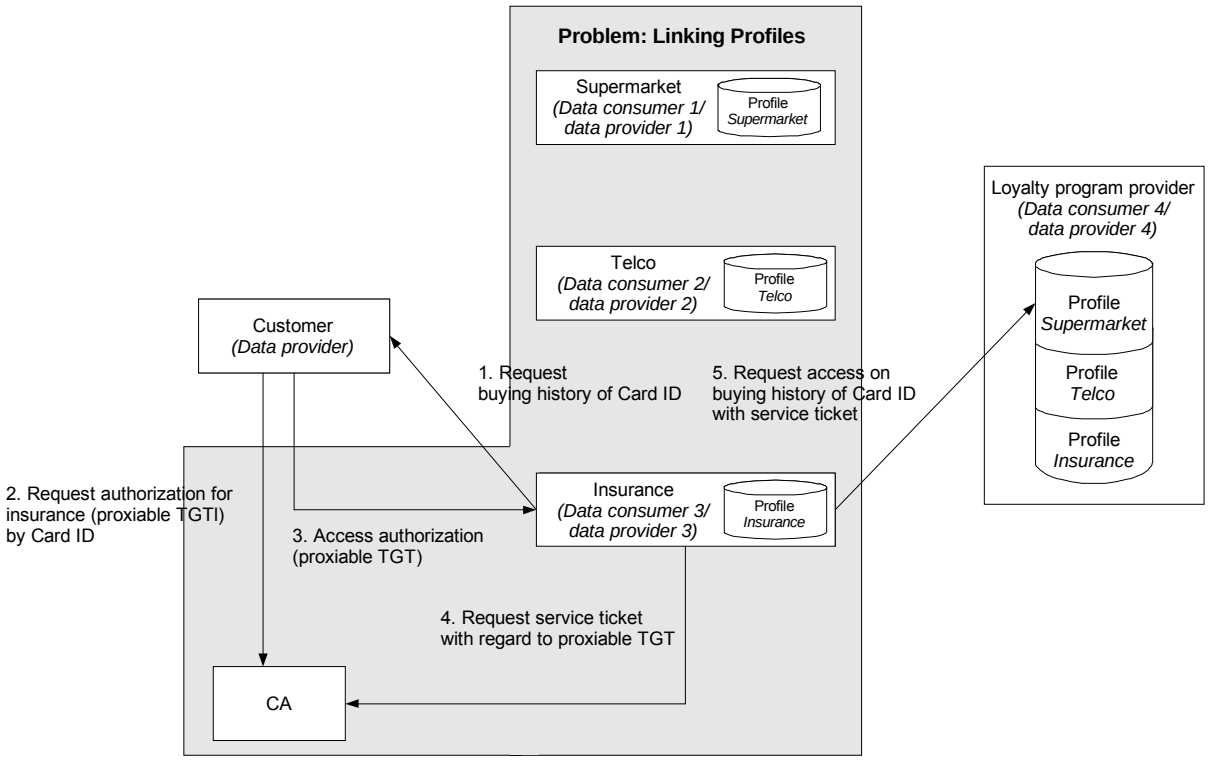

Figure 4.4 Linking customer's profile if Kerberos is applied for delegation of rights.

An approach to prevent such an undesired profiling with delegation of rights in introduced by the usage control mechanism *DREISAM* in chapter six. The application of *DREISAM* to this case study in described in section 6.1.6.

4.5 Case Study: Privacy Threats of Intelligent Software Agents

There are two main types of privacy threats that are posed by the use of ISAs:

1) Threats caused by agents acting on behalf of a user (through loss of control over the activities that are executed to get the right results, through software-errors inside the agent, through the unwanted disclosure of the user's personal information and when an agents runs into a more powerful or an agent in disguise), and;
2) Threats caused by the fact that the ISA is acting on behalf of the user and thus, producing data traces, which may be linked to the user's identity (traffic flow monitoring, data mining and even covert attempts to obtain personal information directly from the user's agent or by entering databases and collecting personal data).

User Profiling

It is this issue of "user profiling" that is at the core of the privacy risk associated with the use of ISAs. Typically, an ISA user profile would contain a user's name, contact numbers and e-mail addresses.

Beyond this very basic information, the profile could contain a substantial amount of additional information about a user's likes and dislikes, habits and personal preferences, frequently called telephone numbers, contact information about friends and colleagues, and a list of electronic transactions performed.

Depending upon the levels of security associated with the user profile and the data, this information has to be secured within the ISA. However, the security of the data residing within the agent is only one part of the concerns regarding privacy.

The more significant concern is the dissemination of information during transactions, and in the general conduct of the agent's activities on behalf of the user.

As an agent collects, processes, learns, stores and distributes data about its user and the user's activities, the agent will possess a wide variety of information which should not be divulged unless specifically required for a transaction. In the course of its activities, an agent could be required, or be forced to divulge information about the user that he or she may not wish to be shared.

The most important issue here is one of openness and transparency. As long as it is clear to the user exactly what information is being requested, what purpose it is needed for, and how it will be used (and stored), the user will be in a position to freely make decisions based on informed consent.

Of even greater concern is the situation where the ISA may not be owned directly by the user but is made available to the user by a service or by an organisation in order to assist in accessing one or more services.

Resuming, the user is required to place a certain degree of trust in the agent – that it will perform its functions correctly as requested. However, this trust could well come with a very high price tag, one that the user may have no knowledge or awareness of – the price to his or her privacy.

The challenge is to employ a ISA that independently performs its tasks, while fully preserving the privacy of the persons involved, up to the level specified by the persons themselves. The

agent should for that purpose be able to distinguish what information should be exchanged in what circumstances to which party.

4.6 Conclusion

Business processes are becoming increasingly oriented to the interests of a customer. In addition to the collection of personal data, its delegation and usage by service providers in place of the customer as far as further service providers are concerned is necessary. The use of personal data leads, however, to privacy problems that are considered to be an important acceptance factor. Privacy is violated when a customer's data is collected, processed, stored or delegated without his consent. Service providers desire an accountability of their customers though so that transactions can be related to them and they can be identified in the case of fraud. In the following chapter, process models for introducing privacy in business processes are introduced and the suitability of identity management as a security mechanism for private data in single-stage and multi-stage business processes is investigated.

5 Privacy-aware Business Process Design and Identity Management

Inventing privacy in business processes is the aim of this chapter. A general approach is presented by the Enterprise Privacy Architecture in order to identify business processes which make use of customers' personal data or attributes and to implement privacy regulations via privacy policies in an information system of a service provider. One suggestion towards a data protection certification is presented by section 5.2. Section 5.2 proposes to apply process models for security in information and communication security for data protection. Section 5.3 investigates on current identity management system whether they preserve informational self-determination in single-stage and multi-stage business processes. The security properties of current identity management systems concerning disclosure of personal data and the security requirements for a self-determined use of disclosed personal data are introduced in section 5.4. Section 5.5 shows an exemplary case study where attributes are used by means of anonymised credentials in order to get access on services. Section 5.6 summarises the results of this chapter.

5.1 Privacy-aware Business Process Design by an Enterprise Privacy Architecture

There is no viable technology that enables consumers to enforce proper use of their personal information throughout an enterprise. As a consequence, customers are required to trust an enterprise once they disclose their personal data. However, enterprises willing to implement fair privacy practices usually face the following problems:

- Business processes are designed without considering privacy requirements. Thus, enterprises are forced to create stockpiles of personally identifiable information (PII or short personal data) instead of collecting personal data when needed for the business at hand.
- Existing services often identify users even though their identity is not needed for the business at hand. Privacy-enhancing security technology that provides security with less data is rarely used.
- Enterprises store a variety of personal data. Larger enterprises may not know what types of PII are collected and where it is stored.
- Enterprises may neither know the consent a customer has given nor the legal regulations that apply to a specific customer record.

From above we conclude that enterprises that want to respect the privacy of consumers need three main technologies:

- Privacy-enabling design,
- privacy management services, and
- privacy-enabled security services.

Privacy-enabling design includes techniques making services more privacy friendly. A core building block is data minimisation. The goal of data minimisation is to minimise the amount of personal data than needs to be collected to achieve the objectives of an enterprise. This

includes privacy-enabling applications that are designed to provide services with least the amount of data needed. Tools for such applications are pseudonymity systems and anonymous authentication schemes.

Even with privacy-enabled design, an enterprise still stores a certain amount of personal data. Therefore customers are required to trust the enterprise to use this data as promised in a privacy policy. *Privacy management services* help enterprises to enforce the promised practices in an auditable way. Thereby privacy policies have to define the allowed access and use of personal data as collected by the enterprise, stored in different systems, and used by its business applications.

Without computer security, a company cannot guarantee privacy. *Privacy-enabled security services* are needed to secure the infrastructure running the enterprise privacy management services. Nevertheless, existing security technology often provides security without privacy. Examples are non-anonymous identification and authentication schemes, data collected by intrusion detection systems, and coarse access control. In order to enable privacy, these technologies need to be transformed into privacy-enabling security services. Analogously to privacy-enabled applications, the goal is to provide security without collecting personal data about honest users.

In the remainder of this section, we introduce the IBM Enterprise Privacy Architecture (EPA), a methodology for enterprises to provide an enhanced and well-defined level of privacy to their customers. A more detailed description can be found in (Karjoth, Schunter and Waidner, 2002).

5.1.1 The IBM Enterprise Privacy Architecture

The IBM Enterprise Privacy Architecture is a methodology that allows enterprises to maximise the business use of personal information while respecting privacy concerns and regulations. It provides a sustainable privacy management system, which can be customised to the total set of privacy regulations and privacy choices facing an enterprise. It includes privacy-friendly business processes, privacy-enabling security technology, and enterprise privacy management. Privacy-friendly business processes are derived from ordinary business processes by minimizing the data needed to provide the desired services. It may include switching to equivalent service alternatives that require less personal data. It may also utilise privacy-enabled security technology.

A unique aspect of EPA is that it provides an analysis of privacy in the context of real business processes by stripping privacy down to its most essential form of actors, rules and data. This is accomplished via object modelling techniques that compile a picture of privacy flows where obligations, risks and opportunities can be clearly identified. This analysis also provides clear linkage to identify which privacy enhancing technologies are appropriate and provides the raw data necessary to customise technology implementations.

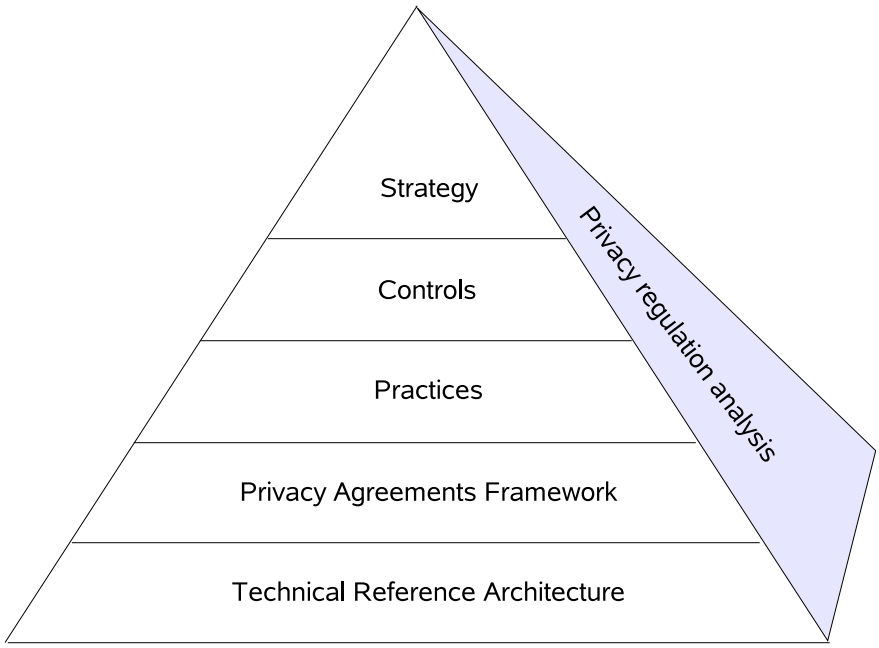

Figure 5.1: Building blocks of the IBM Enterprise Privacy Architecture

EPA introduces privacy-awareness and privacy services into enterprises in a systematic and complete way. Figure 5.1 illustrates its components, outlined in form of a pyramid. As a prerequisite, the EPA privacy regulation analysis identifies and structures the applicable regulations. The Management Reference Model (top 3 layers in Figure 5.1) constitutes the tip of the EPA pyramid, defining the privacy strategy and practices of the enterprise. The Privacy Agreements Framework provides a privacy-enabled model for privacy-enhanced business process re-engineering. The lowest layer is the Technical Reference Architecture that defines the technology for implementing the required privacy services.

5.1.1.1 Privacy Regulation Analysis

Regulatory compliance is a primary driver of privacy-related activity in the marketplace. Thus, it is clear that a useful picture of the regulatory landscape is a pre-requisite to developing any kind of privacy architecture. The challenge is that regulations are typically written in dense legal style with formats and terminology that tend to differ depending on their origin and purpose.

EPA addresses this challenge by regulatory summary tables and regulation rules tables. Regulatory summary tables summarise the applicable regulations using a unified terminology. The regulation rules tables identify data that is in the enterprise as well as the legal restrictions on using such data. The regulation rules tables are enterprise-specific and more formal than the regulation summary table. An entry describes which party can perform which action on which type of data, the resulting privacy obligations, and a reference to the legal regulation. In addition, the four business-use phases Collection, Retention, Processing and Use (“CRPU”) are used to categorise the scope of privacy regulations.

5.1.1.2 Management Reference Model

The EPA Management Reference Model addresses the enterprise-wide processes necessary for a comprehensive privacy management program. These processes are structured and linked to drive the program starting from a strategic view down through the implementation of privacy practices (see Figure 5.1).

Strategy defines the privacy philosophy, the high-level policies and identifies the applicable regulations. This represents the highest level of an enterprise's privacy program and embodies its philosophy, its policies and the regulations it will adhere to. The outputs are a privacy strategy as well as a security strategy. Both define what an enterprise will do for protecting privacy and security.

Control defines the general controls necessary to enforce policy. Its components are a Privacy Requirements Process, the Information Asset Classification and Control, a Compliance Enforcement Process, a definition of the Organisational Roles and Responsibilities as well as an Employee Education Program.

Practices defines the incorporation of policy into business processes. This represents the level of an enterprise's privacy program that translates privacy policy obligations into the general processes, programs and activities that will implement them. Its components are a Privacy Statement declaring the enterprise policy, a Customer Preference Program for defining opt-in and opt-out choices, an Individual Participation Process that enables customers to access their data, a Dispute Process, an External Communication Program that advertises the privacy efforts of an enterprise, and Information Access Controls that protect the enterprises' data and resources.

5.1.1.3 Privacy Agreements Framework

The Privacy Agreements Framework models the transaction level management of privacy at the points where enterprises use personal information within business processes. This includes processes that connect the individual to the enterprise, processes linking people and departments within the enterprise, and processes linking the enterprise with third parties. This model can then be used to identify privacy agreements that are required between the players involved. The main parts of the model are players, data, and rules.

The *players* are the entities that interact while processing collected data. Basic players are data subjects (persons about whom data is collected) and different data users (enterprises or employees using the data). The player model uses an object-oriented modelling technique to identify the players, their operations on the data, as well as the interactions among the players. The result is documented using UML class and collaboration diagrams.

The *data model* identifies the data needed for the processes. Besides identifying the fields collected in forms, it classifies data into at least three categories:

- Personally identifiable information is the most sensitive kind of information that can be linked to a real-world identity. Examples include a tuple name/surname or a U.S. social security number.

- Depersonalised Information is PII where the identifying information has been replaced by a pseudonym. Even though this data is less sensitive, some parties are able to re-personalise it by replacing the pseudonym with the identifying information. Examples include the age with a customer number.
- Anonymised Information contains no identifying information or pseudonyms. It is the least sensitive kind of information that can be obtained by removing all personal data from a set of data. For anonymised data, it is required that identifying the data subject given the data is virtually impossible. Examples include the town of residence or an age in years on its own (i.e., without any other information that may enable identification of the data subject).

The *rules model* identifies the rules that govern the usage of data by players and their operations. It defines what player may perform which operation for what purpose. In addition, rules may impose conditions and may define obligations that result from performing an operation.

5.1.1.4 Technical Reference Architecture

To guarantee that an enterprise provides sufficient privacy to its customers, privacy-enforcement needs to be deployed on an enterprise-wide scale. All applications that handle personal data need to make sure that the handling adheres to the promised policies. An enterprise-wide privacy-management system uses at least three types of systems:

- The *Policy Management System* enables the administrators of the system to define, change and update privacy policies. It distributes the privacy policies to the privacy enforcement systems.
- The *Privacy Enforcement System* enforces the privacy protection for each individual resource that stores privacy-relevant data. It obtains policies from the policy management system and offers auditing data to the audit console. The privacy enforcement system is usually split into two parts: A resource-specific resource monitor shields the resource and a resource-independent authorisation director evaluates the policies and decides whether requests are granted or not. The authorisation director authorises operations on the collected data. After evaluating the policy, the authorisation director returns whether the request is authorised or not and whether an authorised request implies any privacy obligations. Each kind of protected resource (database, CRM system, etc.) uses a corresponding resource monitor. This monitor shields the resource from direct access. Each incoming request is translated into a call to the authorisation director. Only if the authorisation director authorises the request, the request is forwarded to the resource. The resource monitor records audit data and tracks pending privacy obligations.
- The *Audit Console System* enables the Privacy Officer to review the audit information stored in the enforcement nodes and the policies distributed by the policy management systems. Audit services help organisations evaluate regulatory compliance and develop corporate privacy policies.

The EPA Technical Reference Architecture may be refined by a fine-grained privacy authorisation language that enables enterprises to formalise and enforce privacy practices and to manage the consent of their customers.

5.1.2 Other Privacy Architectures

Surprisingly, there are not many approaches that provide a unified approach to a privacy-aware business process design. The International Security, Trust, and Privacy Alliance (ISTPA) has published a Privacy Framework11 for the protection of personal and organisational data, which defines security, privacy, and trust services and their relationship. It provides an open, policy-configurable model consisting of 10 integrated privacy services and capabilities, which can be used as a template for designing solutions and supporting audit assessments covering security, trust, and privacy requirements.

5.2 Compliance in Enterprises – How can Trends in IT-Security be transferred to Data Protection?

Continuous and repeated tasks in organisations in the private as well as in the public sector exist quite often. Important areas are among others:

- Sales and Customer Relationship Management (CRM)
- Production Planning (PP), Production Management (PM)
- Logistics and transportation
- Financial management
- IT Service Management (ITSM)
- Total Quality Management (TQM)
- Information Security Management (ISM)

In many of these areas good practice process models are used that suggest standardised proceedings for typical organisations. These process models are meant to be used as framework – they need to be adapted to the specific needs and environmental conditions of the organisation. For data protection no generic good practice process models have been suggested so far. In this chapter a good practice model for data protection is introduced and explained. This contribution bases on an article by (Meints, 2007).

5.2.1 Requirements for Data Protection Management

Data Protection Management (DPM) in an organisation has to take a number of influencing factors into consideration:

- Legal grounds for data protection include concrete operational requirements such as the maintenance of an inventory of procedures in which personal data are processed. In addition they contain general principles that need to be implemented in the specific context of the organisation and the corresponding procedures.
- Processing of personal data typically is supported or completely done using Information and Communication Technologies (ICT). Thus a strong link to the fast changing ‘state of the art’ in ICT is given.
- In addition DPM needs to take into consideration changing conditions within the organisation.
- Currently there is no metric for defined levels of data protection.

11 http://www.istpa.org/index.cfm

- As a consequence of all these influencing factors no static and long time persistent level of data protection in organisations exists.

Many of the tasks in DPM are of continuous nature. In this case very often cyclic processes are used.

5.2.2 Forerunner Process Models for DPM

Looking at the described requirements especially three areas in which good practice process models are used show significant similarities to DPM. They are:

- Total Quality Management (TQM), e.g. ISO 9000
- IT Service Management (ITSM) and IT Governance, e.g. IT Infrastructure Library (ITIL)[12] and CobiT[13]
- Information Security Management (ISM), e.g. ISO/IEC 27001 and 17799

In these process models especially two cyclic process models commonly are used:

- The Deming Cycle for quality management, named after William Edward Deming (U.S. American consultant and mathematician) including the steps “Plan, Do, Check, Act”
- The lifecycles of ICT supported procedures including the steps “Plan, Build, Run”

[12] ITIL is an IT Service Management Framework developed since mid of the 1980s by the British Central Computer and Telecommunications Agency (today Office of Government Commerce, OGC). Information about ITIL can be found on the web pages of the IT Service Management Forum (ITSMF) via http://www.itsmf.org.

[13] CobiT was developed since 1995 by the U.S. Information Systems Audit Control Association (ISACA) as an integrated IT-governance framework and currently is available in the version 4.0. Download: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981.

The following figure shows these generic process models.

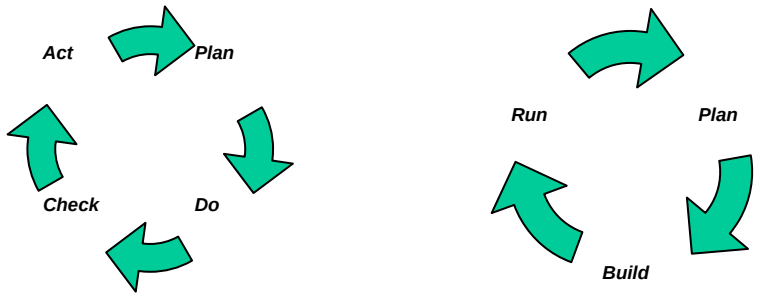

Figure 5.2: Deming Cycle and lifecycle of ICT supported procedures.

Especially Information Security Management Systems (ISMS) developed since mid of the 1990s show a close proximity to DPM. ISMS typically include a good practice management model and corresponding management tasks (e.g. British Standards[14] and CobiT[15]) or catalogues of ICT security risks and corresponding countermeasures (Baseline Protection Catalogues[16]). The good practice process models have in common that they cover (a) the strategic layer of planning in enterprises (by policies), (b) mid term planning (tactical level) by concepts and (c) the operational level by concrete technical and organisational measures. In Germany especially Baseline Protection is established in the private as well as the public sector. For this reason the DPM process model was developed in close accordance to the Baseline Protection information security process model.

5.2.3 The DPM Process Model

The DPM process model consists of two parts: a core process which is accompanied by a number of supporting processes. This process model was developed in close accordance to Baseline Protection to show potential synergies with the corresponding IT-security management process. The following figure shows the DPM core process (left) in comparison with this security management (core) process (right).

[14] The British Standards were developed since mid of the 1990s as IT security management system by the British Standards Institute (BSI). Currently part 1 and part 2 are standardised also as ISO/IEC 27001 and ISO/IEC 17799. Information is available via http://www.bsi-global.com/Global/iso27001.xalter.

[15] Control Objectives for Information and Related Technologies (CobiT) is an Information and Communication Technology (ICT) governance framework developed by the U.S. Information Systems Audit Control Association (ISACA) in 1995. The current version is V 4.0. Further information is available via http://www.isaca.org.

[16] Baseline Protection is a method developed since 1994 by the German Federal Office for Information Security (BSI). Since January 2006 Baseline Protection consist of three standards (BSI 100-1, BSI 100-2 and BSI 100-3), which are also part of ISO/IEC 27001, and the Baseline Protection Catalogue. For further information and downloads see http://www.bsi.de/gshb/index.htm.

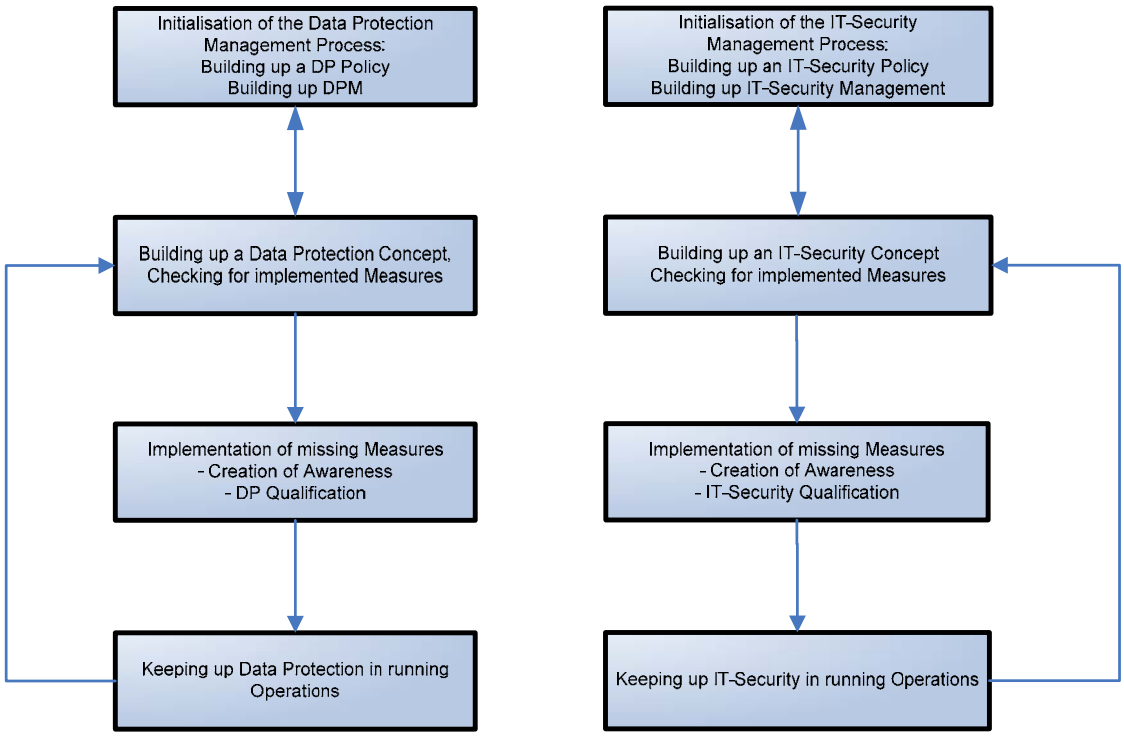

Figure 5.3: Data Protection Management Process (left) and Baseline Protection IT-Security Management Process (right).

The DPM core process starts with the assumption that an organisation is introducing DPM as a new process. For this reason the process starts with the strategic level of building up a data protection policy. Strategic targets of an organisation with respect to data protection can be for example:

- Excellence in data protection as a unique selling proposition on the market
- Compliance to data protection legislation on a minimum level

Also in the strategic level the data protection process is built up.

On the tactical level activities around the data protection concept are carried out. This includes

- Preparation of the list of procedures in which personal data are processed (also called inventory of procedures)
- Compiling the legal grounds that need to be taken into consideration
- Documentation of the list of measures for each of the procedures; currently a catalogue of generic measures corresponding to the German data protection law is in preparation. It is planned to include this list in the next version of the Baseline Protection Catalogue.
- Checking the status of implementation for these measures

In the next step missing measures are implemented, user awareness for data protection is created and qualifications of employees of the organisation with respect to data protection are carried out.

The following process step includes keeping up the reached level of data protection in running operations. Supported by a number of sub-processes (cf. Figure 5.4) this process restarts the core process in case significant changes require this, leading to a cyclic process model. The strategic level of the core process needs to be repeated in cases of fundamental changes only. Though the targets of the DPM process (i.e. compliance to data protection legislation) and the IT-security process (i.e. the required level of confidentiality, integrity and availability) differ, these processes can be used in close accordance.

The following Figure shows the main supporting processes:

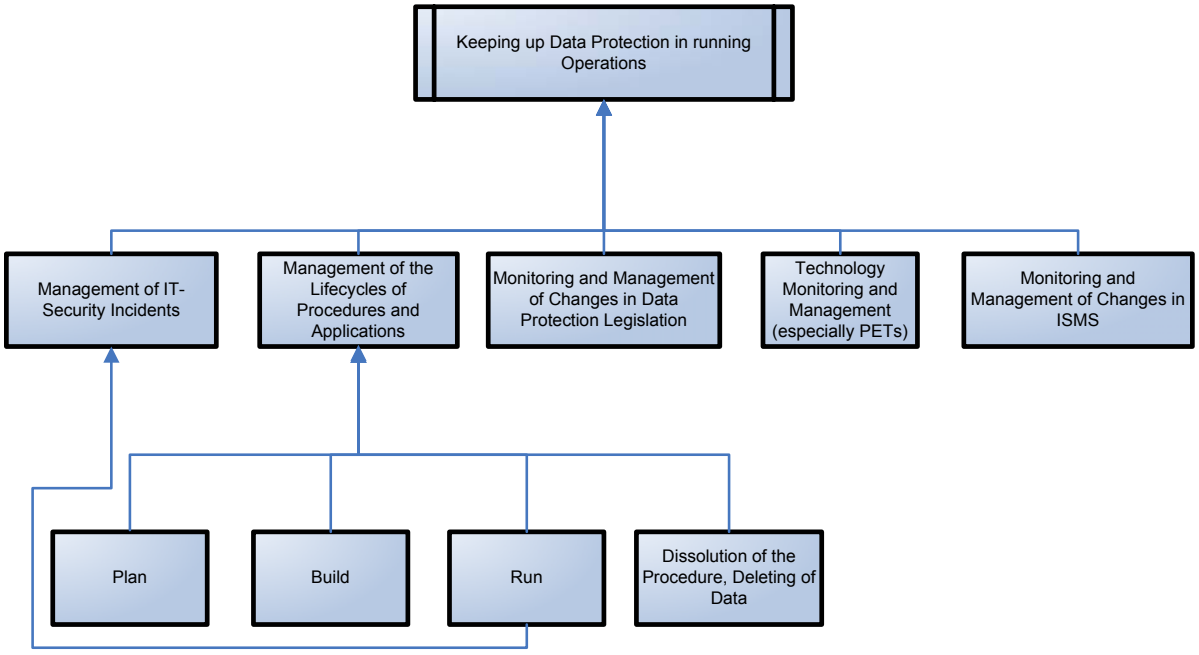

Figure 5.4: Good Practice Supporting Process for the DPM Core Process.

The supporting processes have two functions: (1) implementation of specific data protection related tasks in running governmental or business procedures and (2) triggering of the restart of the central process in case fundamental changes in the environment took place. The main supporting processes are:

- Management of IT-Security Incidents: This especially means taking care of data protection specific aspects such as legal consequences of these incidents and support in dealing with them.
- Management of the Lifecycles of Procedures and Applications: In this context the responsible person (data protection officer or Privacy Commissioner) keeps track of procedures and deals with specific data protection related requests submitted by the operators and users e.g. with respect to information about personal data, deletion etc. These requests in running operations also may result in the initialisation of the IT-

Security Incident Management Process. In addition to the typical model of lifecycles this task does not end with the dissolution of the procedure as possibly longer time spans for deletion of personal data need to be taken care of.

- Monitoring of changes in data protection legislation: Substantial changes require a restart of the cyclic core process.
- Technology monitoring and management, especially with respect to Privacy Enhancing Technologies (PETs): Mature PETs need to be taken into consideration when planning a new procedure or a new version of an existing procedure as they document a change in state-of-the-art of technology.
- Monitoring and management of changes in the Information Security Management System (ISMS) used in the organisation: Fundamental changes in ISMS can mean a change in state-of-the-art of security management and may have an impact on the modelling of the DPM. (Visa versa this is not necessarily the case, change in the DPM may not necessarily result in changes in the ISMS.)

5.2.4 Summary and Outlook

For data protection management no integrated good practice processes have been suggested so far. Basing on good practice process models for information security management in this chapter a first suggestion for a good practice process for data protection management is introduced and explained. An integration of this process model into the next version of the data protection chapter of the Baseline Protection Catalogues (former Baseline Protection Manual) as a German national extension is planned by the Data Protection Commissioners in Germany, in co-ordination and supported by the German Federal Office for Information Security (BSI).

5.3 Business Processes and Identity Management

David Chaum introduces the idea of identity management in 1985 (Chaum, 1985). He considers privacy threats by undesired information flow and abuses while customers authenticates themselves towards service providers and introduces an approach for identification by digital pseudonyms and credentials for certified personal data. Therefore, an unique and verifiable identification of a customer is possible which prevents at the same time undesired data collection and linkability of the collected data. Verification of a customer's identity is achieved by using credentials. The meaning of a credential is a certified statement based on a customers' "*relationship with organisations that are, in general, provided to other organisations*" (Chaum, 1985). Organisations would profit by the small amount of customer data which has to be protected against abuse. Additionally, a customer remains identifiable by using Chaum's system. Furthermore, David Chaum proposes a personal mobile device, a card computer, for a customer who stores customer's pseudonyms and credentials in a protected storage.

Nowadays, the development of identity management systems aims from two sides. Scientific developments, such *Dresden Identity Management (DRIM)* of the TU Dresden (Kriegelstein, 2002), as *iManager* of the University of Freiburg (Jendricke and Gerd tom Markotten, 2000; Wohlgemuth, Jendricke, Gerd tom Markotten, Dorner and Müller, 2004), and of the anonymous credential system of Stefan Brands (Brands, 2000) as well as of the system of Jan Camenisch and Anna Lysyanskaya *IBM idemix* (Camenisch and Lysysanskaya, 2001; Camenisch and Van Herreweghen, 20002) aims primarily at customer's privacy. Industrial

developments, such as *Liberty Alliance* (Liberty Alliance, 2005), *Microsoft .NET Passport* (Microsoft, 2003), and *Security Assertion Markup Language (SAML)* (Maler, Mishra and Philpott, 2003) standardised by *Organization for the Advancement of Structured Information Standards (OASIS)* aims primarily at a authentication system for a *Single-Sign On (SSO)*[17]. An identity management focusing both on *SSO* and on privacy is *Shibboleth* (Carmody, Erdos, Hazelton, Hoehn, BobMMorgan, Scavo and Wasley, 2005; Dors, 2005) by the consortium *Internet2*.

All identity management systems are based on existing public key infrastructures (PKI) for issuing and verifying credentials. Whereas a certification authority (CA) takes up an additional role depending on the identity management system. The main tasks of a CA are to certify statements of customers, issue credentials with respect to these statements, and revoking them. Concerning identity management systems such as *Microsoft .NET Passport*, *Shibboleth*, and *Liberty Alliance*, a CA also manages personal data of their customers. This means that a CA securely stores customer's data and discloses them upon request of service providers and according to customer's privacy policy. Such a CA is called identity provider.

The aim of this section is to investigate on current identity management systems whether they prevent undesired profiling in single-stage and multi-stage business processes in combination with the security interests of service providers towards accountability. Current identity management systems are classified by the role of a CA and customer's trust in it with respect to his privacy. Identity management systems either use one CA as an identity provider, e.g., *Microsoft .NET Passport* and *Shibboleth*, several CA as identity providers for different domains, e.g., *Liberty Alliance*, a common CA, e.g., *iManager*, and a CA without mandatory trust of customers, e.g., *IBM idemix*. In the following, the mentioned identity management systems are examined as representatives of these identity management classes. An exception is *Microsoft .NET Passport*. *Microsoft .NET Passport* does not preserve customer's privacy. Each customer has a global unique identifier. Furthermore, a service provider will get access on the complete customer's data at the global CA upon request.

5.3.1 Single-Sign On with One Identity Provider: *Shibboleth*

Shibboleth is a web-based identity management system with one identity provider which issues credentials for his customers. It aims at a SSO of customers and an attribute exchange of customer's data to service providers. A customer logs on an identity provider. Afterwards, a customer does not need to log explicitly on other service providers, since this identity provider confirms this authentication to service providers by a credential. This credential contains also the requested customer's data, if the customer has agreed to this attribute exchange. A customer is able to act with pseudonyms and to decide on the disclosure of personal data while the access control is managed by the identity provider on behalf of a customer. *Shibboleth* is based on the standard *SAML V1.1* (Maler, Mishra and Philpott, 2003) and presumes a web browser without any extensions. The following investigation on *Shibboleth* concerning it as a security mechanism for private data is based on its specifications (Carmody, Erdos, Hazelton, Hoehn, BobMMorgan, Scavo and Wasley, 2005; Dors, 2005).

[17] SSO means that a customer authenticates at one service and this service further authenticates this customer implicitly to other services in the same domain (Garman, 2003).

5.3.1.1 Model and Authentication Protocol

The participants of the model are customers, an identity provider, service providers, and optional a lookup service called *WAYF* (*Where are you from?*). *Shibboleth* supports two variants for authentication and attribute exchange: *Browser/Post* and *Browser/Artifact* protocol.

A customer is identified by his name and disclosed personal data. These data are managed by one identity provider who is part of the trust domain of this customer. An identity provider certifies statements about the identity of a customer by means of attribute certificates (credentials). So, an identity provider takes up the role of a certification authority. Service providers trust an identity provider that this identity provider certifies customer's identity according to his certification policy. The identity of a customer is protected against unauthorised access by the identity provider. This is a presumption for a controlled disclosure of personal data by the customer. A service provider offers a web-based service and protects it by an access control. Based upon the identity of a customer, a service provider gives or denies access to his service to a requesting customer. The centralised lookup service *WAYF* is used, if a service provider does not know the address of the identity provider. This service redirects the authentication request of a service provider to customer's identity provider.

The protocol variants *Browser/Post* und *Browser/Artifact* differs in the kind of attribute exchange. Regarding the *Browser/Post protocol*, a service provider receives customer's data by means of a credential which has been issued by the identity provider of the corresponding customer. Regarding the *Browser/Artifact protocol*, a service provider receives a token by the customer. By using this token, a service provider is allowed to get access on customer's data at his identity provider. Both variants are adopted from *SAMLV1.1* and extended by the *WAYF* service. The protocol variant *Browser/Post* as specified in (Carmody, Erdos, Hazelton, Hoehn, BobMMorgan, Scavo and Wasley, 2005) is described in the following. Figure 5.45shows the message flow of this protocol. The dashed flows and the use of the *WAYF* service are optional. As the message flow shows, the identity provider of a customer is involved in each authentification and attribute exchange.

Step 1 request a service of a service provider by a customer. The customer uses a web browser for his service request. Step 2 represents the authentication request of a service provider to his customer. If the address of customer's identity provider is not known to this service provider, the authentication request is posed to the *WAYF* service. The *WAYF* service redirects this request to the identity provider of this customer in step 3. Otherwise, the request is posed directly to the corresponding identity provider. Step 4 asks the customer to log on at his identity provider, if he has not already done it. The customer uses a secret token, e.g., a password, for his authentication towards his identity provider. This secret token is solely known to him and his identity provider. The identity provider certifies the identity of the customer for the requesting service provider in step 5. The result is either a credential or an error message. Latter is sent, if the customer could not authenticate himself. Step 6 and 7 realise the attribute exchange between a customer and the requesting service provider via the identity provider. Therefore, the service provider proves his authorisation by the credential which he has got in step 5. A disclosure of customer's attributes is done with respect to the negotiated policy between the customer and his identity provider. Based on the credential and customer's data, the service provider grants or denies access to his services to the requesting customer in step 8.

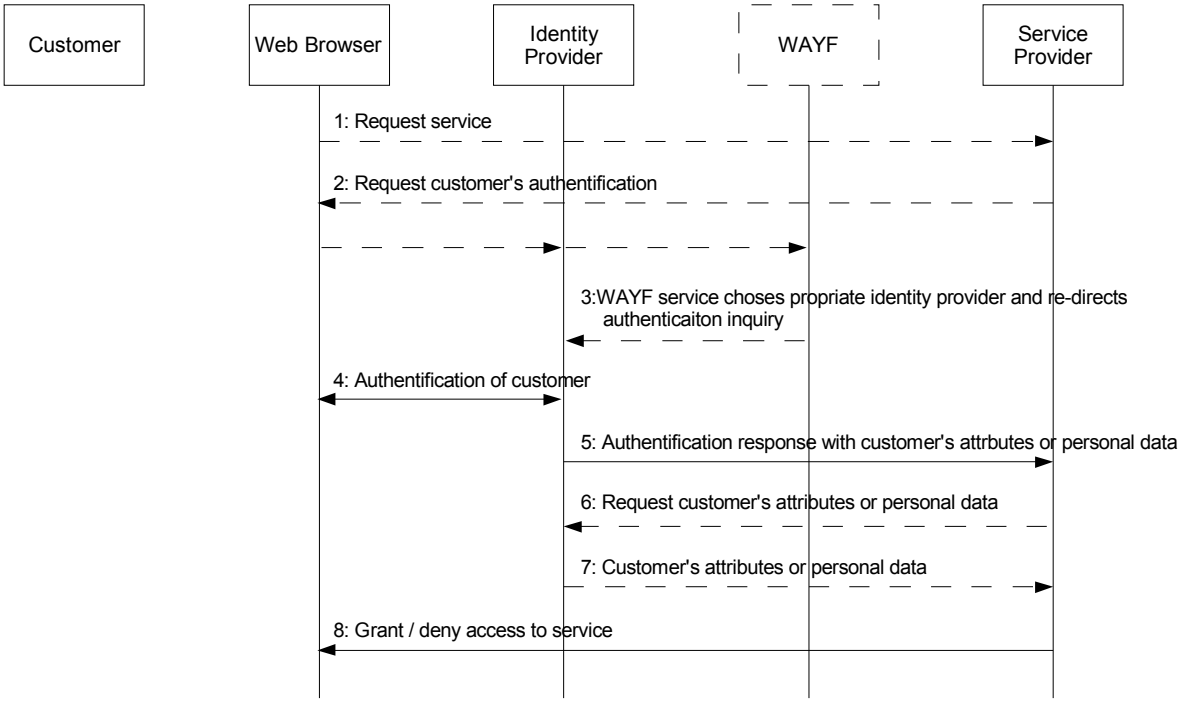

Figure 5.5 Authentification by using the Browser/Post protocol of Shibboleth.

5.3.1.2 Applying *Shibboleth* on Multi-Stage Business Processes

Shibboleth does not consider an authentication and attribute exchange of a customer to service providers via his proxy in multi-stage business processes. The application of *Shibboleth* in multi-stage business processes is shown in Figure 5.6. The authentication of customer's proxy is done in step 5. So that a proxy is able to prove a specific identity of a customer towards a subordinate service provider, the proxy needs the corresponding credential. The identity provider issues such a credential but only if the proxy is able to prove his authorisation for the access on customer's data. The only possibility for a proxy to get a credential to customer's data is to authenticate as his customer. Therefore, the proxy needs to use the secure authentication token of his customer towards the corresponding identity provider. A delegation of this secret authentication token to his proxy results in an unrestricted access for his proxy on customer's identity. This proxy could modify the privacy policy of the customer and abuse customer's identity for own purposes. By using the transcript of a protocol run, it is not possible to distinguish whether a customer or his proxy has used a given identity of the customer. Consequently, a customer loses control on the disclosure of his identity, if he delegates his secure authentication token to a proxy. Additionally, a proxy becomes a "Big Brother", since he has access to all pseudonyms and personal data of the customer. Therefore, he is able to retrace all transactions of this customer. A complete profiling is possible. Finally, privacy is only preserved in multi-stage business processes, if the customer trusts his proxy with respect to the negotiated use of his delegated secure authentication token. But this is a contradiction to the assumption of an untrustworthy proxy, as assumed in the threat analysis of section 2.

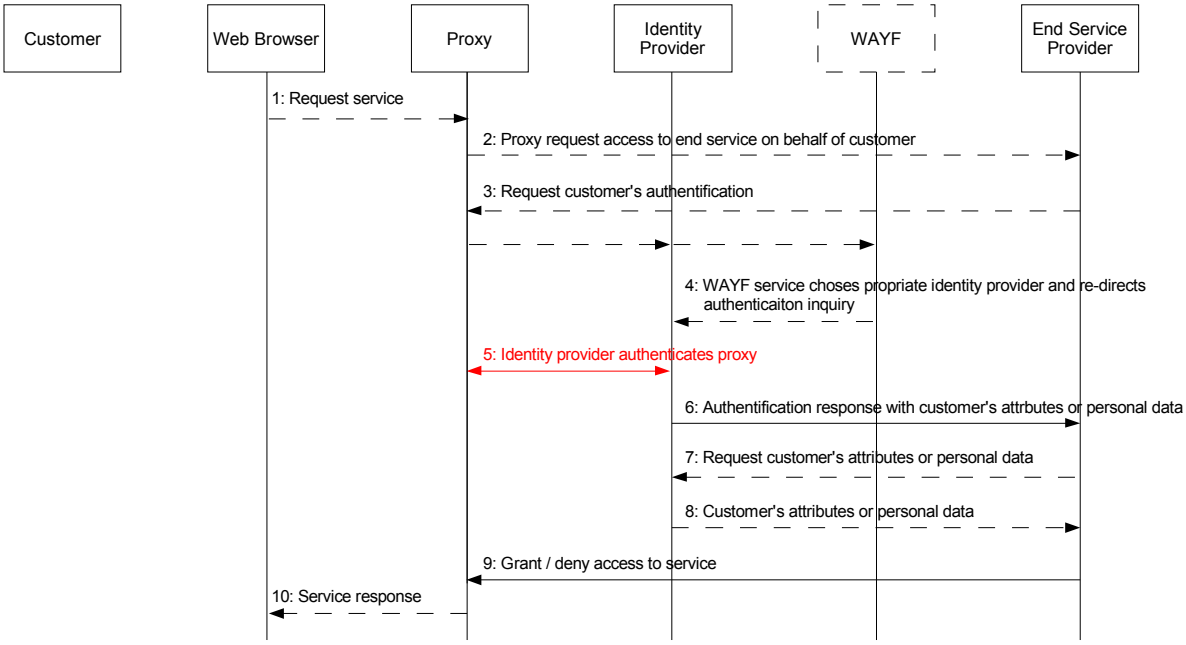

Figure 5.6 Applying Shibboleth on a business process with one proxy.

5.3.1.3 Security Properties of *Shibboleth*

The specification (Carmody, Erdos, Hazelton, Hoehn, BobMMorgan, Scavo and Wasley, 2005) considers a man-in-the-middle attack on the communication between the participants of the protocol. This attacker aims to get knowledge about customer's data and to intercept a credential in order to use it for impersonation. The specification proposes the use of a digital signature as a countermeasure for impersonation attacks. *Shibboleth* has the following security properties with respect to privacy of customers and accountability interests of service providers:

- **Secure data storage:** The specification assumes a directory service according to *LDAP* for storing customer's data. *LDAP* supports the use of an access control on the managed data (Yeong, Hows and Kille, 1995).
- **Situation-dependent disclosure of personal data:** A customer is able to decide on the disclosure of his personal data to service providers by his privacy policy. His identity provider grants and denies access to customer's data according to his privacy policy. But the grammar for his privacy policy is not defined in the specification of *Shibboleth*. Additionally, the protocol specification does not consider an interaction between a customer and his service provider with respect to an attribute request during a protocol run. So, a customer is not able to decide ad hoc on the disclosure of personal data.
- **Unlinkability of transactions:** Shibboleth supports the use of pseudonyms, especially of transaction pseudonyms. A pseudonym is the value of the credential attribute <saml:NameIdentifier> in lieu of the customer name which is used for an authentication at the identity provider. By using transaction pseudonyms, customer's transactions seem to be independent with respect to the customer. However, since the identity provider of a customer is involved in each authentication, the identity provider knows all customer transactions and is able to

create a profile. A customer has to trust his identity provider that the identity provider does not publish or delegate this knowledge about his customer.

- **Authentification without showing identifying data:** Customer's data are disclosed by means of a credential. These data are a by the credential attribute called <saml:AttributeValue xsi:type="xsd:anyURI"> ... </saml:AttributeValue>. *Shibboleth* does not limit the type and values of attributes. Therefore it is possible for an identity provider to certify a property of customer's data instead of their values which may unambiguously identify a customer.
- **Non-repudiation of customer's transactions:** A customer proves his identity towards his identity provider by his secure authentication token. Thus, only the owner of this token, the given customer, is able to give a valid proof of his identity. Based on a valid authentication proof, an identity provider certifies the identity of this customer towards a requesting service provider. Therewith a relationship exists between a given transaction of a customer and to the identity of this customer. An identity provider is able to show this relationship.
- **Revoking customer's anonymity in case of fraud:** Since an identity provider knows the relationship between the identity of a customer and his pseudonyms which are used by the customer in his transactions, an identity provider is able to revoke the anonymity of a customer in case of fraud.

However, *Shibboleth* does not support authorisation for an access on customer's data which could be delegated to a proxy. As the application of the authentication protocol on multi-stage business processes shows, a customer would have to delegate his secure authentication token to his proxy. It follows that a customer would lose control on his identity, since a proxy would have unrestricted access on customer's identity by using this authentication token. Consequently, privacy is only preserved as long as *Shibboleth* is used in single-stage business processes.

5.3.1.4 Conclusion

By using the identity management system *Shibboleth*, a customer is able to preserve his privacy against undesired identification, profiling, and linkability of his transactions by deciding on the access on personal data. Since the identity of a customer is managed by solely one identity provider and all authentication of a customer are carried out via his identity provider, this identity provider is able to create a complete profile about his customer. It is not possible for a customer to control the use of this knowledge at his identity provider. Therefore, a customer has to trust his identity provider with respect to the use of his identity.

This mandatory trust relationship will have to be extended to customer's proxy, if *Shibboleth* is used in business processes with proxies. *Shibboleth* does not consider a usage control on disclosed customer's data and consequently is not suitable as a security mechanism according to customer's privacy interests in multi-stage business processes.

5.3.2 Single-Sign On with Several Identity Providers: *Liberty Alliance*

Liberty Alliance (Liberty Alliance, 2005) is also a specification for a web-based identity management system similar to *Shibboleth*. The aim of *Liberty Alliance* is Single-Sign On and an attribute exchange between customers and service providers via one or more identity

providers. A customer is able to decide whom to give his personal data according to the situation. A situation is thereby defined by the URL of the given service. The specification consists of two parts: *Liberty Identity Federation Framework (ID-FF)* specifies the basic system for an SSO with pseudonyms in different application domains (*Circles of* Trust), and *Liberty Alliance Web Services Framework (ID-WSF)* as the extension for an attribute exchange and delegation of authorisations to service providers for an access on personal data. The classification of service providers and identity providers with respect to their application domain and the use of delegable authorisations are two main differences to *Shibboleth*. The aim of this section is to investigate on the identity management system of *Liberty Alliance* in order to identify its security properties concerning privacy interests of customers and security interests of service providers.

5.3.2.1 The Authentication Model of *Liberty Alliance*: *Circle of Trust*

The authentication model of *Liberty Alliance* focuses on a classification of identity providers with respect to their application domain. The tasks of an identity provider are certification of customer's identities, management of these identities, authentication of customers towards service providers, and a confidential treatment of the knowledge about customer's transactions. Application domains are defined depending on the trust and business relationships between service providers and identity providers. An application domain is called *Circle of Trust*. All identities of a customer for a given *Circle of Trust* are managed by the corresponding identity provider of this *Circle of Trust*. A login of a customer to an identity provider or to a service provider leads to an implicit logon to all service providers within this *Circle of Trust*. The relationship of different identities of a customer with in a *Circle of Trust* is called *federated network identity* (Cantor, Hodges, Kemp and Thompson, 2005).

Figure 5.7 shows two examples for a *Circle of Trust*. A customer uses two different identities for the application domains *mobility* and *spare time*. These two identities are disjunctive. Concerning the domain shopping, customer's identities for the services *car dealer*, *insurance*, and *finance* are managed by the identity provider *government*. The identity provider *myCity* manages customer's identities for the services *free e-mail*, *sports*, and *ticketing* of the application domain *spare time*. It is assumed that these identity providers also manage the personal data of a customer with respect to these applications. The identity providers *government* and *myCity* do not know a priori that the partial identities *car holder* and *spare time* belong to the same customer. A customer is able to distribute his identity to different identity providers and to divide one "Big Brother" in many "Big Brother" with less knowledge about the customer.

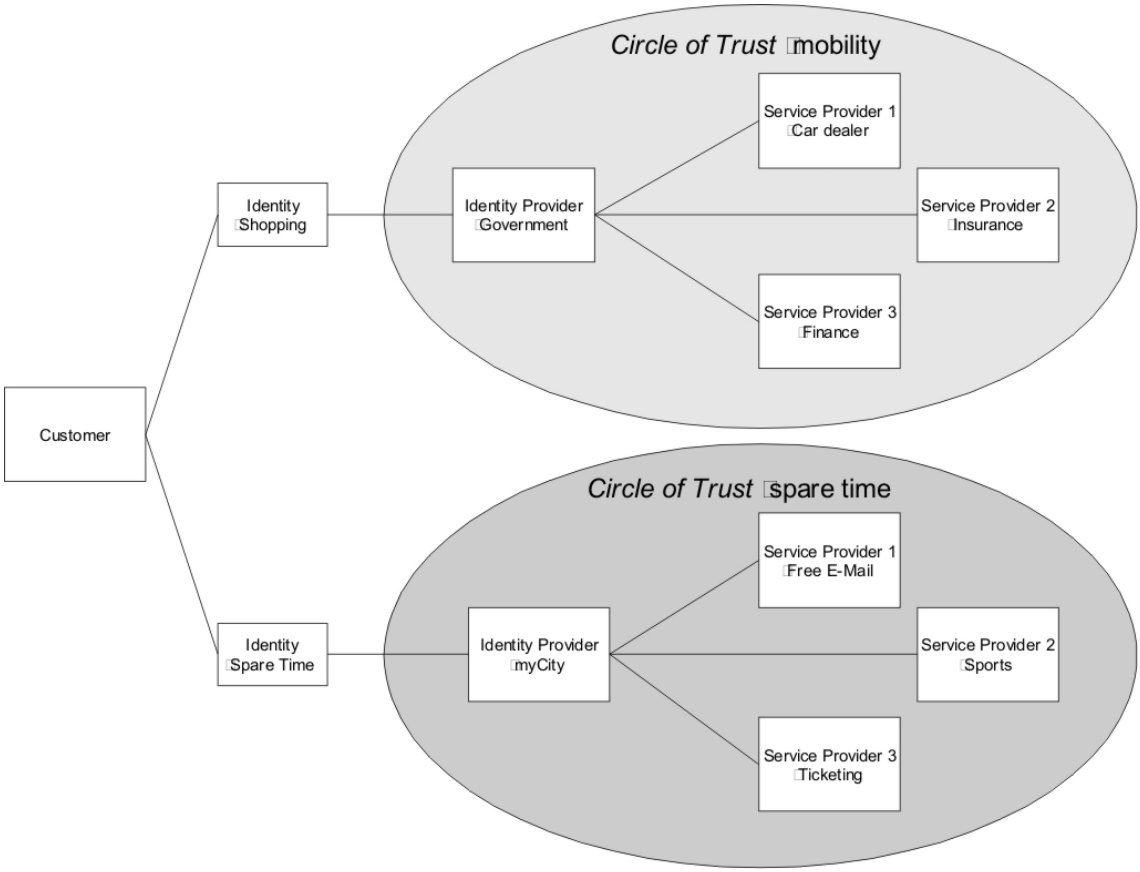

Figure 5.7 Distributing an identity to different identity providers for two *Circles of Trust*.

5.3.2.2 The General Single-Sign On Protocol of *Liberty Alliance*

Liberty Alliance specifies a general authentication protocol in order to realise a SSO. Based on this protocol, the protocols *Liberty Artifact Profile* for an exchange of a link to a credential of a customer, *Liberty Browser POST Profile* for an exchange of customer's credential, and *Liberty-Enabled Client and Proxy Profile* for a redirect of an authentication request from one identity provider to another identity provider of different *Circle of Trust* are derived (Aarts, Kavsan and Wason, 2005). The general authentication protocol, as shown in Figure 5.8, has the following properties:

- **Involvement of an identity provider in all transactions within a *Circle of Trust*:** All authentication requests of service providers to a customer within a given *Circle of Trust* are redirected to the corresponding identity provider. Thus, an identity provider is involved in each transaction of a customer with respect to a given *Circle of Trust*. This has an effect on the trust relationship between a customer and his identity provider with respect to the use of this knowledge: if a customer is not able to control the use of this knowledge by an identity provider, the customer has to trust his identity provider with respect to its use according to the negotiated policy.
- **Web browser as client software:** This authentication protocol and its derivatives are based on the web protocols HTTP and SSL. A web browser without extensional

functionality, such as Java or plug-ins, is sufficient for the use of this identity management system by customers.

- **Certification of an identity by a credential:** An identity provider certifies the relationship between personal data and a customer by a credential. This credential is valid within the corresponding *Circle of Trust*. The grammar for a *Liberty Alliance* credential is derived from the standard *SAML V1.1*.

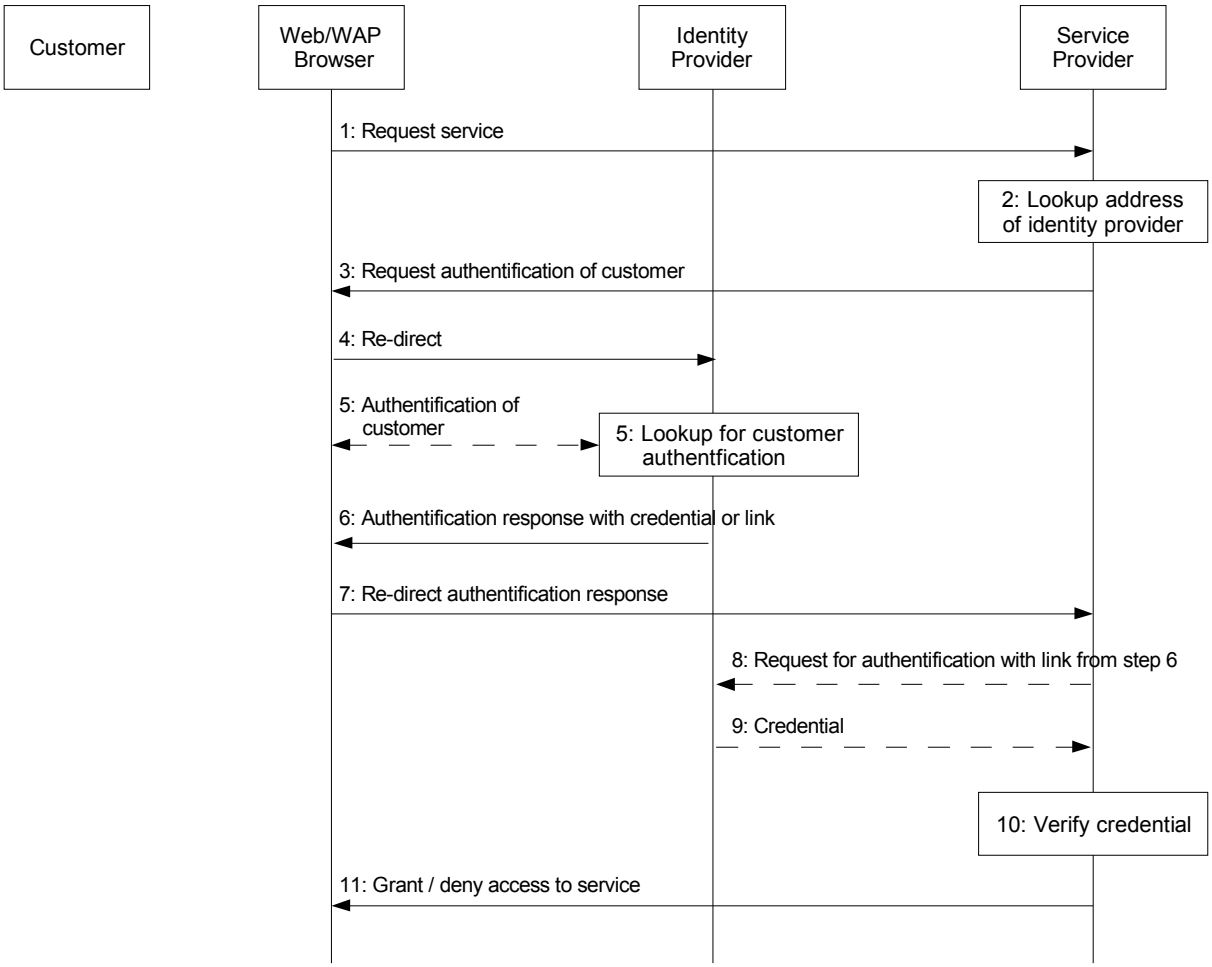

Figure 5.8 Authentification of a customer by using the general authentication protocol of *Liberty Alliance*.

A customer requests a service of a given service provider in step 1. Step 2 determines the address of the appropriate identity provider with respect to the current *Circle of Trust*. Step 3 requests the authentication of this customer by a service provider. This request is re-directed by the web browser of the customer to his identity provider in step 4, since an identity provider is responsible for an authentication response. This identity provider assigns the authentication requests to a customer. If this customer has not already proven his identity to his identity provider, the identity provider requests this customer for authentication in step 5. If the customer has proven his identity successfully, his identity provider responds in step 6 to

the authentication requests of step 4 with the result of customer's authentication. The result is either a credential of the customer consisting of his personal data with respect to the authentication request or a link to such a credential. This response is re-directed to the requesting service provider via the web browser of the customer in step 7. If the response is a link to a credential, step 8 and 9 are executed and the service provider gets this credential from the identity provider. Step 10 verifies the obtained credential. Depending on the authentication response, the service provider either grants or denies access to the requested service in step 11.

5.3.2.3 Access on Customer Data by an Authorisation

An exchange of customer's data to service providers is carried out by a special service type called *Data Services Template* which complies with a directory service. Its specification (Angal, Cahill, Feng, Gourmelen, Kannappan, Kellomaki, Kemp and Sergent, 2005) defines a data model and an application interface for lookup and modification requests. This specification assumes that a data service protects customer's data against an unauthorised access by an access control. If a service provider wants to have access on some customer's data, he has to show his authorisation for the desired access. *Liberty Alliance* defines three use cases for showing an authorisation: a direct inquiry of the service provider at the customer, an indirect inquiry via an interaction service (Kemp, Madsen, Sergent and Whitehead, 2005), and a delegation of an authorisation from an identity provider to the requesting service provider (Aarts, Canales-Valenzuela, Cantor, Hirsch, Hodges, Kemp, Linn, Madsen, Sergent and Whitehead, 2005).

A direct inquiry is in fact a single-stage business process. Both a service provider and a data service provider interact directly with the customer. Figure 5.9 shows the interactions between these three participants.

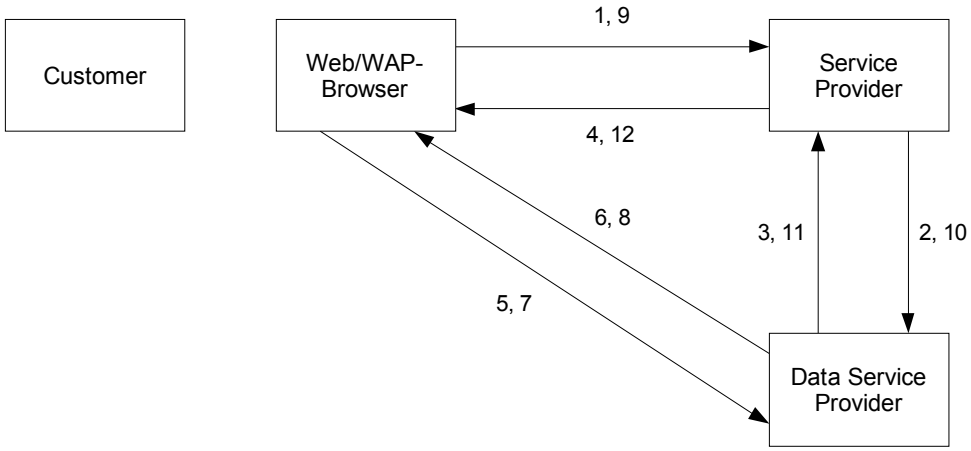

Figure 5.9 Authorisation of a customer with respect to access on his data according to a re-directed d inquiry of a service provider.

A customer authenticates towards a service provider and requests a service in step 1 by an authentication protocol of *ID-FF*. This service provider asks for some personal data of the customer stored by the data service provider in step 2. It is assumed that the service provider

knows the address (URL) of this data service provider. Steps 3 to 5 re-direct this request to the customer. The customer decides on the access requests and thereby on the disclosure of his required personal data in step 6. The customer also shows his identity to the data service provider in step 6, too. This authentication is also carried out by an authentication protocol of *Liberty Alliance*. The data service provider receives the response of the customer in step 7. If the customer agrees to the desired access, the response in step 7 is the desired authorisation. Step 8 and 9 are a kind of acknowledgment together with the authorisation and gives the execution of this transaction back to the service provider. In step 10 repeats the service provider his request together with the authorisation of the customer to the data service provider. The data service provider checks the authorisation and, if it is valid, returns the requested personal data of the customer to the service provider in step 11. The customer gets the results of the data request in step 12.

5.3.2.4 Access and Use of Customer Data in Business Processes with Proxies

The other uses cases for an attribute exchange represent a multi-stage business process. In the second use case, an indirect inquiry and delegation of an authorisation, an interaction service provider takes up the role of a proxy. An interaction service is either carried out by the requesting or a third service provider. Figure 5.10 shows the interactions of an inquiry for data access via an external interaction service provider.

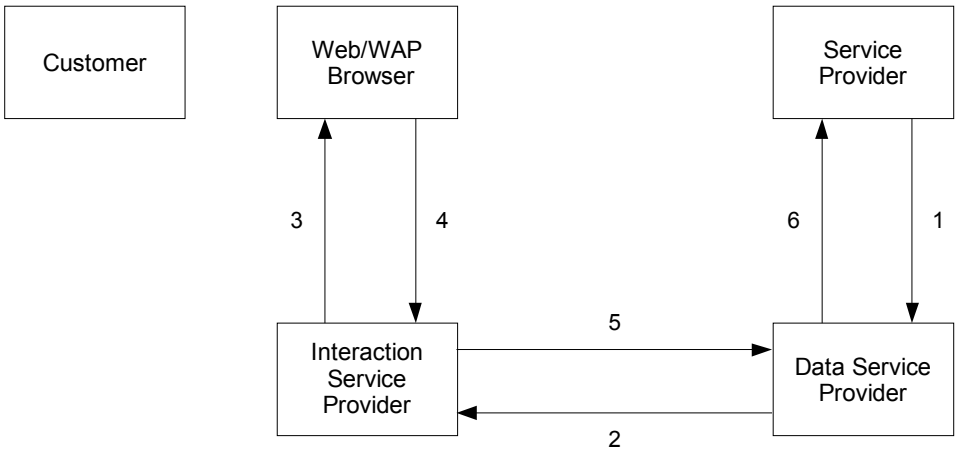

Figure 5.10 Delegation of an authorisation for an access on customer's data to a service provider via an interaction service provider.

Step 1 corresponds to the request of a service provider to some personal data of a customer. A request is re-directed from a data service provider via an interaction service provider to the customer in step 2 and 3. A request consists of the URL of the data service provider, an informal description of the request, a URL of the request, and the request itself. A customer responds to the request in step 4. Since his response is re-directed via the interaction service provider, the interaction service provider gets to know the response. Thereby, the interaction service provider is a man-in-the-middle and as a proxy re-directs the delegates the response of the customer to the data service provider. Is the authorisation available to the data service provider, this provider discloses the requested personal data according to this authorisation in

step 6 to the requesting service provider. The customer signs his authorisations optionally with his private key sk_U.

The third use case for an attribute exchange represents a delegation of an authorisation by means of a credential which has been issued by an identity provider of the customer. This identity provider confirms that a given service provider is allowed to act as a proxy of the customer towards another, so called, end service provider. By such an authorisation, a service provider is allowed to get access on customer's data or to use customer's data for a specific purpose. An end service provider trusts an identity provider that this identity provider issues authorisation according to his certification policy. A credential representing an authorisation is extended by attributes concerning the delegation participants and the purpose of a delegation. The statements of a delegation concern the identity of the customer and his proxy, latter by his public key pk_{Proxy}, the transaction identifier (TID), and the point of time when this credential has been issued. The statements concerning the purpose of a delegation relate to a service of a specific end service provider, given by a URL.

Furthermore, *Liberty Alliance* supports a delegation of an authorisation via several service providers. A delegation chain arises. The first node of a delegation chain is the service provider with whom a costumer interacts directly; the last node is the service provider who shows a delegated authorisation to the end service provider. In case of a transitive delegation, a delegation chain with at least two nodes, a credential for a proxy is extended by the nodes of the delegation chain. Thereby, an end service provider is able to reconstruct the certification chain by the delegation chain which is necessary to verify the credential of the requesting service provider. It is possible to restrict a transitive delegation in time and in the succeeding service providers respectively nodes. Liberty Alliance assumes that an end service provider will follow these restrictions, if he verifies a delegated credential. A transitive delegation via two service providers is shown in Figure 5.11.

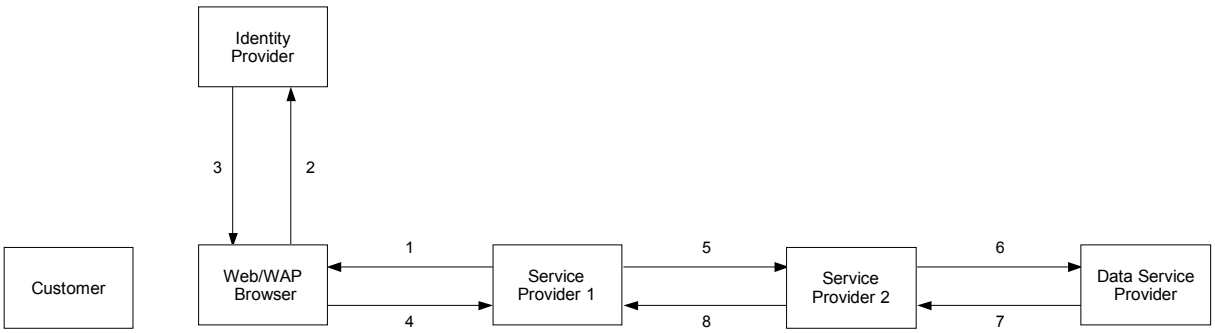

Figure 5.11 Delegation and use of an authorisation with respect to an access on customer's data via a delegation chain of two nodes.

In step 1 asks *service provider 1* for an authorisation on behalf of *service provider 2* in order to get access on some personal data of the customer which are stored at a data service provider. Step 2 re-directs the request to the identity provider of the customer who issues the credential with this delegation chain according to the privacy policy of the customer. By steps 3 and 4, *service provider 1* gets the requested credential and forwards it in step 5 to *service provider 2*. In step 6, *service provider 2* requests access on customer's data and shows the

delegated credential. The data service provider verifies the credential and grants or denies the access. Step 7 to 8 returns the result of this transaction to *service provider 1*.

But *Liberty Alliance* does not specify a protocol for the delegation of authorisations as a credential. Gomi, Hatakeyama, Hosono, and Fujita extend *Liberty Alliance* by a protocol specification for a delegation of authorisations (Gnomi, Hatakeyama, Hosono, and Fujita, 2005). Their approach is similar to Kerberos (Kohl and Neuman, 1993). Nodes in a delegation chain are seemed to be trustworthy with respect to customer's privacy. Their protocol is not part of the current *Liberty Alliance* specification.

5.3.2.5 Security Properties of *Liberty Alliance*

The identity management system of *Liberty Alliance* realises an access control on the identity of customers. Additionally, this system supports a usage control by an authorisation concerning an access on customer's data and using customer's data for authentication of a proxy. The specification of the basic system *ID-FF* recommends using SSL or TLS in order to protect the communication channels with respect to accountability, integrity, and confidentiality of the messages between the participants. The security properties of *Liberty Alliance* with respect to disclosure and use of customer's data and to accountability of customer's activities are as follows:

- **Secure data storage:** Personal data of customers which are stored by a data service provider are protected against unauthorised access [Aar2005b]. Since a customer is not able to control whether a data service provider enforces the access control according to his rules, a customer has to trust the data service provider.
- **Situation-dependent disclosure of personal data:** *Liberty Alliance* refers to the principle of data economy during an authentication of a customer towards service providers. A customer is able to decide on the disclosure and thereby on the access on personal data. The implementation guideline of *ID-FF* (Kemp, Aarts, Bone, Castellanos-Zamora, Crom, Kannappan, Lindsay-Stewart, Maeda, Meyerstein, Nochimowski, Gonzalez, Poignet, Serret, Vanderbeek, Vittu, Walter, Sergent, Madsen, Cahill, Linn, Landau and Sibieta, 2005) recommends to respect customer's privacy interests by a policy which is managed by an identity provider and followed in case of SSO. By using a privacy policy, a customer is able to decide on the use of his pseudonyms and to get informed when they have been used. The statements of a policy refer to a service provider. Depending on a service provider, a customer is able to specify his policy and thereby the use of his pseudonyms with respect to a transaction. But a customer has to trust his identity provider, that this provider follows the privacy policy of the customer.
- **Delegation of the minimal authorisation:** A customer is able to specify the data types of the requested personal data in an authorisation. A request contains the requested data as attributes of type <InquiryElementType>. An authorisation picks up these attributes in combination with the decision of the customer. Depending on customer's decisions, a data service provider grants access on these data. If an interaction service provider is used, an authorisation is not mandatory protected against modification. To ensure the integrity of an authorisation, *Liberty Alliance* recommends protecting an authorisation by a digital signature.

Since neither an inquiry nor the response of a customer is encrypted, an interaction service provider will get to know the information flow from this customer to the given service provider. Additionally, an interaction service provider is able to modify customer's authorisation and use it for own purposes by replacing the name of the authorised service provider with his own name, if the authorisation is not digital signed. In this case, the least privilege of an authorisation cannot be guaranteed. The specification of an interaction service points these threats and a mandatory trust of customers in an interaction service provider out [Kem2005a]. In order to identify an abuse, a logging of an inquiry by all participating service providers and the customer is recommended but is not followed up.

- **Unlinkability of transactions:** The basic system *ID-FF* considers personal data as customers' pseudonyms. By using pseudonyms, linkability of customers' transactions by service providers is hindered. A pseudonym for a customer is either created by a service provider and federated with the identity by the corresponding identity provider or by an identity provider. Transaction pseudonyms are also possible and are implemented by a random number. The involved identity provider is able to link the transactions of his customers because of his involvement in each authentication of his customers.

A customer can also act with a pseudonym in a delegated authorisation. His pseudonym, given by the credential attribute <saml:NameIdentifier>, is encrypted by the pubic key of the end service provider and so cannot be read by his proxies. But, since the trust model of Liberty Alliance assumes untrustworthy service providers with respect to privacy, an end service provider would share his knowledge about customer's pseudonym with the other service providers. Thus the encryption is useless.

If a delegated authorisation refers to an access on personal data, the mapping of a pseudonym to the corresponding data record at a data service provider must be identifiable for the data service provider in order to decide on the access inquiry. Consequently, a data service provider is also able to link customers' transactions if they need access on those personal data which is stored by this provider. Profiling is possible. It follows that a customer has to trust his data service provider with respect to the enforcement of his access control and to the confidential treatment of his knowledge about customer's transactions.

- **Authentification without showing identifying data:** The response of an identity provider depends on the inquiry of a service provider and on the consent of the corresponding customer. If a service provider needs identifying data of a customer, this customer has to agree on this inquiry, if he wants to use this service. In this case, an authentication without showing identifying data is not possible.
- **Non-repudiation of customer's transactions:** Accountability of a customer to an identity respectively pseudonym is guaranteed by customer's authentication with a secure authentication token to his identity provider in step 5 of the general authentification protocol. An identity provider establishes accountability of customers for a given *Circle of Trust*. In case of a delegated authorisation, both customer and his proxy are given in the credential within the attribute `SessionContextStatement`. A proxy is given as a `ProxySubject` (Aarts, Canales-Valenzuela, Cantor, Hirsch, Hodges, Kemp, Linn, Madsen, Sergent and Whitehead, 2005). If an authorisation is available as credential, then it is protected by the digital signature of an identity provider.

- **Revoking customer's anonymity in case of fraud:** Depending on the application domain, the identity provider of the correspondent *Circle of Trust* is able to revoke the anonymity of a customer due to his involvement in each customer's transaction within this *Circle of Trust.*

Usage of customer's personal data for authentification is specified by an authorisation. An authorisation may be represented by a credential. *Liberty Alliance* has the following properties concerning a usage control of customer's data:

- **Reference to purpose of an authorisation:** The purpose of an authorisation with respect to a business process is given by the attribute ResourceAccessStatement. The purpose is given by the identifier of the customer and the proxy as well as the URL of the requested service.
- **Restricted delegation of an authorisation:** An authorisation can be delegated via several service providers forming a delegation chain. A delegation chain for personalised services in a multi-stage business process is defined as ProxyTransitedStatement in a credential.
- **Revocation of an authorisation:** *Liberty Alliance* does not consider a revocation of a delegated authorisation.
- **Integrity of an authorisation:** If an authorisation is implemented by a credential, then its integrity is protected by the digital signature of the credential issuer. In case of a direct inquiry for an authorisation, the issuer is the customer. Otherwise it is the identity provider of the customer. In case of a direct delegation of an authorisation from a customer to the requesting service provider and in case of an indirect delegation via an interaction service provider, the integrity of an authorisation is not as default protected.
- **Enforceability of an authorisation:** *Liberty Alliance* assumes that end service providers follow the conditions of an authorisation. But a customer is not able to control this. Consequently, a customer has to trust end service providers with respect to the enforcement of these conditions. In case of an interaction service provider, its specification (Kemp, Madsen, Sergent and Whitehead, 2005) proposes to create a transcript of the protocol run with all participants in order to verify the proper use of an authorisation afterwards by, e.g., an audit (Canales-Venezuela, Ellison, Hodges, Kellomäki, Kemp, Linn and Thompson, 2005).

Liberty Alliance supports a delegation of personal data of customers to proxies in order to get access on further services. However, *Liberty Alliance* assumes trustworthy service providers with respect to the enforcement of authorisation's conditions. But this assumption contradicts with the assumptions in the trust model of *Liberty Alliance* with respect to privacy. The trust model assumes untrustworthy service providers except identity providers which are seemed to be trustworthy. Consequently, *Liberty Alliance* does not preserve privacy in multi-stage business processes.

5.3.2.6 Conclusion

The identity management system of Liberty Alliance enables customers to protect their privacy against threats of single-stage business processes, e.g., undesired identification,

profiling, and linkability of their transactions. This is done by an access control on personal data of customers which is enforced by identity providers and data service providers. However, a customer has to trust these services that they do not share their knowledge about him without his consent.

Regarding the use of disclosed personal data, Liberty Alliance specifies a use by authorisations. However, *Liberty Alliance* assumes trustworthy service providers with respect to the enforcement of authorisation's conditions. But this assumption contradicts with the assumptions in the trust model of *Liberty Alliance* with respect to privacy. The trust model assumes untrustworthy service providers except identity providers which are seemed to be trustworthy. Consequently, *Liberty Alliance* does not preserve privacy in multi-stage business processes.

5.3.3 Identity Management with Partial Identities: *iManager*

The *iManager* is the central security tool of a personal mobile device which is considered to be trustworthy. The *iManager* offers interfaces to the customer, to the security mechanisms, and to the applications of a mobile device. The access to personal data and to cryptographic keys is exclusively possible by using the identity manager. An application's request to these data will be checked by the identity manager whether the customer has given his consent to the publication of this personal data in the current situation.

5.3.3.1 Architecture of *iManager*

The architecture of the *iManager* and its interfaces is shown in the Figure 5.12. Based on a *security platform*, the components *identity configuration*, *identity negotiation*, and *confirmation of action* are responsible for managing the partial identities (Jendricke, 2002).

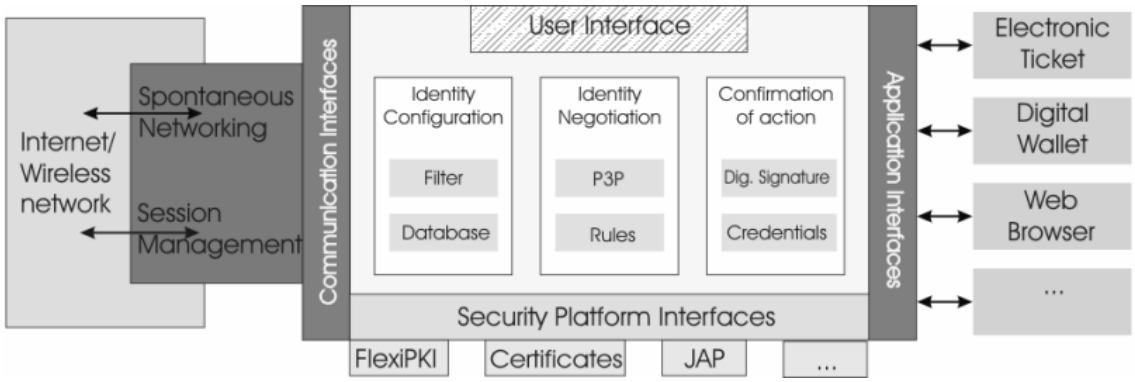

Figure 5.12 Architecture of *iManager*.

The **user interface** has to be comprehensible for security novices, since they are not able to verify and assess the security mechanisms of the *iManager* and therefore a misuse of them leads to a compromise of the security and privacy of the customer. The possibility of a misuse has to be reduced. The acceptance of the security tool also depends on its customer interface. In order to facilitate the use of a security tool, the protection goals of multilateral security (Rannenberg, Pfitzmann and Müller, 1999) have been classified in customer and system controlled protection goals by analyzing their interdependency (Jendricke and Gerd tom

Markotten, 2000). This leads to a reduction of the customer interface complexity. The customer controlled protection goals *anonymity* and *accountability* are configured by partial identities and their choice in a situation. The integration of the *iManager* in the customer interface of the mobile device is shown in the following Figure 5.13. At any time, the customer is able to check his identity.

Figure 5.13 Integration of *iManager* in the graphical user interface of a personal mobile device.

The identity configuration enables a customer to choose and create a partial identity with respect to a current situation. A situation is defined by a communication partner, the current service and current partial identity. Since the anonymity level cannot increase subsequently any partial identity can not be changeable. If the customer wants to change the current partial identity, the iManager checks if the desired anonymity level could be reached with the intended change. Further implemented functionalities are: to edit partial identities, to store them in a secure database on the mobile device, and to recognise the current situation. The secure database stores partial identities and customer's security, his privacy policies and rules for the security tools. A filter checks the data flow of the mobile device and it is possible to fill a web form according to P3P with respect to a suitable partial identity and customer's permission.

Figure 5.14 Solving a conflict by choosing the appropriate partial identity.

An **identity negotiation** is necessary, if a service needs more data from the customer than he wants to publish in this situation. This conflict can be solved with a negotiation between this service and the customer. A restricted automatically negotiation is possible by the implementation of P3P and consequently the comparison from the service's and customer's security and privacy policy. In case of a conflict, *iManager* informs the customer of this conflict and proposes solutions like a suitable partial identity for solving it. For example, in the scenario a customer wants to buy an electronic railway tickets and wants to get some premium points. For the premium points, the virtual ticket automat requests some personal data of the customer. A conflict occurs since the customer acts with his partial identity *anonymous*. The *iManager* proposes to use the partial identity *traveller* for solving this conflict. The Figure 5.14 shows this case.

The customer decides his accountability and the accountability of his communication partner for each partial identity. The component **confirmation of action** implements the accountability of the customer by a digital signature tool. It is used whenever a digital signature is required, e.g. for self-signing personal data. Since the customer declares explicitly his intent, he signs with his handwritten signature and authorises the digital signature tool to sign the corresponding credential. The digital signature key is selected by choosing the suitable partial identity. By this means, the technical functions of the key management will be shown in a more comprehensible manner.

The **security platform** consists of interfaces to cryptographic primitives, anonymity services, to a session management, a secure database, and to security services. Anonymity services are the foundation of identity management, since it enables to customer to be anonymous towards his communication partners. The anonymity service *JAP* (Berthold, Federrath and Köhntopp, 2000) is used for IP networks. For spontaneous networking, a library of the University of Rostock, Germany, (Sedov, Haase, Cap and Timmermann, 2001) is used. The cryptographic primitives for encryption and digital signatures are implemented by the library *FlexiPKI* (Buchmann, Ruppert and Tak, 1999).

5.3.3.2 Certification and Authentification by a Partial Identity

Authentification by a partial identity is based on a credential. A CA certifies the relationship between customer's attributes and his public key pk_U. A partial identity used by the *iManager* consists of personal as well as identifying data of the customer and pk_U. The public key of a partial identity represents the corresponding pseudonym (Jendricke, 2003). A credential is implemented as an X.509 attribute certificate (Farrell and Housley, 2002). The certification and authentification process is as follows:

Figure 5.15 shows the certification process. Protocol participants are a customer with his personal end device including the *iManager* and a certification authority. It is assumed that the CA has authenticated its identity before the protocol start, e.g., via TLS (Dierks and Rescorla, 2006).

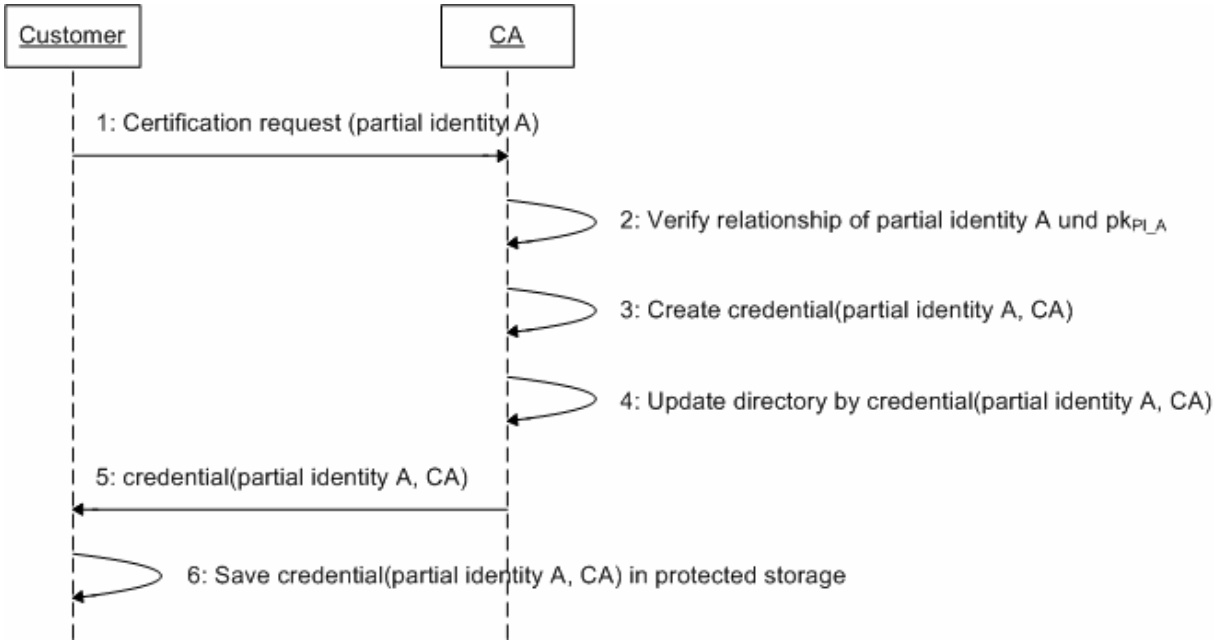

Figure 5.15 Certification of a partial identity.

Step 1 requests a certification of a *partial identity A* by the customer. The CA verifies the relationship of this partial identity to the given pseudonym of the customer (pk_U). This is done out-of-band. If this relationship is authentic, the CA will create a credential consisting of the *partial identity A* and its identity by digital signing it with its private key sk_{CA}. Step 4 stores the resulting credential is the public directory service of the CA. Step 5 returns this credential to the customer. The customer staves it in the protected storage of his personal device and links it to the corresponding *partial identity A* in step 6.

Figure 5.16 shows the authentification protocol for a single-stage business process. It is assumed that the customer acts as default with his partial identity *anonymous*. No identifying data will be disclosed. A service provider needs some data about the customer to offer him his service. These data are summarized as *partial identity b* of the customer. Step 1 request the service of the service provider by the customer. In step 2, the service provider requests some

personal data for his service. The *iManager* recognises this requests and verifies whether the current partial identity (here *anonymous*) allows this service provider to get access on the requested data. So, the *iManager* detects the current situation specified by the identity of the service provider, his service, the requested data, and the current partial identity of the customer. Since the customer acts under his partial identity *anonymous*, there is a conflict between the request and the current situation of the customer. This conflict is shown to the customer in step 4. The *iManager* also propose a suitable partial identity with respect to this situation. In step 5, the customer chooses a solution to solve the conflict which is here the change from partial identity *anonymous* to the proposed *partial identity B*. Step 6 changes the current identity to the chosen *partial identity B*. Step 7 is optional. The protocol continues with step 7 only if the customer has no credential for this partial identity. Otherwise, the *iManager* starts the certification protocol. Step 8 shows the *partial identity B* to the service provider by showing the corresponding credential. The relationship of this credential to the customer is shown by a digital signature with customer's private key sk_{PK_B} with respect to the pk_{PI_B} of this credential. In step 9 the service provider verifies the digital signature of the customer and his credential. Step 10 grants or denies access to the requested service.

Figure 5.16 Authentification of a customer in a single-stage business process by a partial identity.

5.3.3.3 Applying *iManager* on Multi-Stage Business Processes

The *iManager* does not consider multi-stage business processes. Applying the authentication protocol of the *iManager* leads to the situation as shown in Figure 5.17. Steps 1-9 are the same. The difference is in step 10. In order to use customer's personal data of his *partial identity B*, his proxy has to be able to digital sign a message with customer's private key sk_{P_IB}. Therefore, the customer delegates sk_{PI_B} it to his proxy in step 10. But by delegating sk_{PI_B}, the customer loses control on the use of his *partial identity B.*

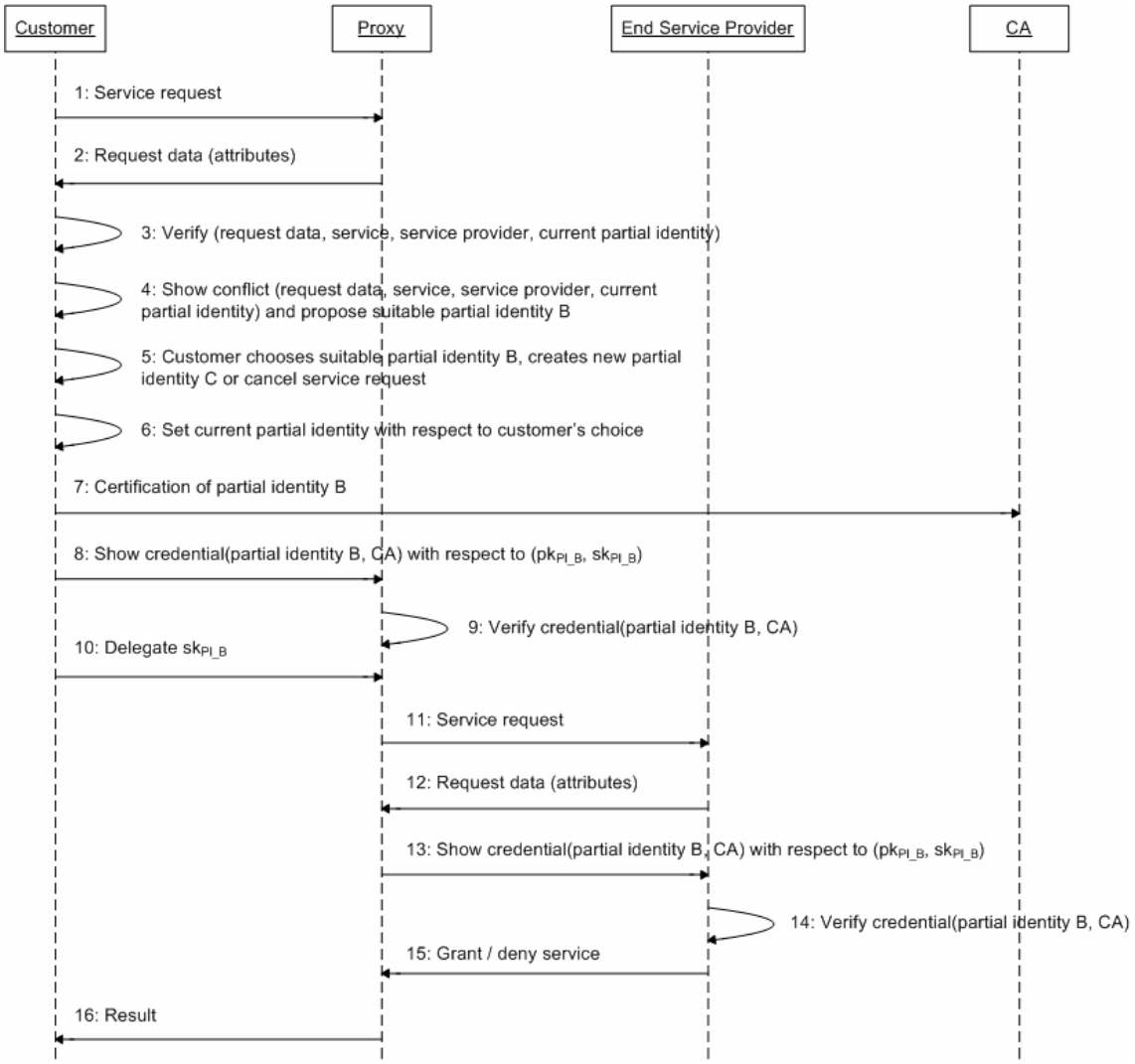

Figure 5.17 Authentification of a customer by his partial identity in a business process with proxy.

5.3.3.4 Security Properties of *iManager*

The *iManager* has been developed for preserving privacy in single-stage business processes. This identity manager empowers his customers to control the access on personal and identifying data by disclosing them via partial identities. The evaluation of its protocols and their application on multi-stage business processes shows the following properties of the *iManager*:

- **Secure data storage:** Personal data and all partial identities of a customer are stored in the protected storage of his personal mobile device. Only the *iManager* has access to it.
- **Situation-dependent disclosure of personal data:** The *iManager* recognises a situation by the current service, service provider, the requested data, and the current partial identity of a customer. A customer discloses personal data and therefore giving access to his data by selecting a partial identity with respect to a situation.

Only the personal data of the selected partial identity will be given to the requesting service provider.

- **Unlinkability of transactions:** The content of a partial identity is defined by a customer. That means that he is able chose whether identifying data is part of a partial identity. Since pseudonyms are part of a partial identity, a customer is able to use services with different identifiers. If two disjunctive partial identities are used for two transactions, these transactions and customer's profiles and service providers seem to be independent with respect to the same customer. But if a customer uses a partial identity also for other transactions, these transactions can be linked by the public key pk_{PI_A} and the digital signature of the customer (cf. to step 8 in the authentication protocol).
- **Non-repudiation of customer's transactions:** In step 8 of the authentication protocol, a customer shows the association of his certifies partial identity by using his correspondent private key sk_{PI_A} for a digital signature. Since a credential is an X.509 attribute certificate issued by a CA, a service provider verifies the authenticity of a partial identity by verifying this credential. By the trust relationship in a PKI to the CA and the digital signature of the CA and of the customer, a transaction is bound to a specific customer.
- **Revoking customer's anonymity in case of fraud:** A CA revokes the anonymity of a customer in case of fraud. As shown in the certification protocol, a CA knows the identity of a customer by verifying the relationship of a partial identity to a customer in step 2.

The *iManager* does neither support storing personal data externally nor a delegation of personal data or partial identities. Consequently, there is no usage control on disclosed personal data. As shown by the application of the authentication protocol on multi-stage business processes, a customer will lose the control on his delegated identity, if he delegates it to a service provider for further use. This service provider is able to impersonate the customer and to trace his past transactions in which the customer has used this partial identity.

5.3.3.5 Conclusion

The *iManager* aims primarily at a usable security tool for mobile security novices in order to preserve their privacy by controlling the disclosure of their personal and identifying data. A customer prevents an undesired identification, data collection and linking of profiles by using disjunctive partial identities, under the presumption that two transactions do not need the same or identifying data of a customer. But in multi-stage business processes, a customer will lose control on his delegated partial identities. Linkability and abuse by impersonation is the consequence.

5.3.4 Anonymous Credentials: *IBM idemix*

IBM idemix (identity mix) (Camenisch and Van Herreweghen, 2002) is an anonymous credential system that is based on protocols for anonymous credentials according to [Cam2001] and requires a PKI. Through the use of anonymous credentials, in his authentication towards service providers and certification authorities a customer is known exclusively by the pseudonym used and the attribute attested by the credential or the data disclosed. The system is used for the identity management system of the EU project *Privacy*

and Identity Management for Europe (PRIME) (Camenisch, Shelat, Sommer, Fischer-Hübner, Hansen, Krasemann, Lacoste, Leenes and Tseng, 2005).

Transactions where the customer uses various pseudonyms appear separately from one another to the customer's communication partner. Even a certification authority that issues a credential for a certain pseudonym does not recognise the same customer again if he verifies the possession of this credential towards the certification authority. The certification authority only knows that the customer possesses a credential with the proven attribute with the applied pseudonym and that this credential was issued by itself. A customer can determine himself with the authentication which personal data of a credential should be disclosed. In addition, *IBM idemix* has accountability mechanisms that allow a disclosure of a customer's identity or the pseudonym of a customer under certain conditions.

IBM idemix is described in the following in excerpts from (Camenisch and Lysyanskaya, 2001; Camenisch and Van Herreweghen, 2002) on the basis of its basic protocols. It is then subsequently examined and evaluated with regard to privacy protection, particularly for a delegation of personal data.

5.3.4.1 The Basic System

The participants in an *idemix-PKI* are customers who receive credentials and identify themselves, service providers and certification authorities who examine and issue the credentials and a de-anonymisation provider who discloses the identity ort he pseudonym of a customer under certain conditions. A customer can therefore receive a credential from a certification authority and identity himself to a service provider with this credential. A credential is always linked to a pseudonym that was previously agreed upon between the customer and the respective certification authority. A credential can contain certain data of the customer, whereby the customer can determine himself on verification of a credential which certified data or its attributes are disclosed.

Initialization and Assumptions

The registration of pseudonyms as well as the issue and examination of credentials take place by interactive protocols between the customer and the respective service provider. A customer U possesses a secret symmetric key k_U to which his entire pseudonyms and anonymous credentials are linked. Certification authorisations and service providers each possess an asymmetric cryptographic key pair (pk_X, sk_X) where X stands for the name of the service provider. A certification authority uses its private key sk_{CA} for issuing a credential. This credential can then be examined with the pertaining public key pk_{CA}. For the verification of a credential, the customer uses the public key pk_{SP} in the protocol with the service provider SP. *IBM idemix* assumes the following:

- The customer does not trust any service provider not to generate a profile about him and without his consent.
- Private communication relationships between customer and service provider are reached as far as third parties are concerned by the use of anonymity services.
- A service provider authenticates himself towards the customer for each communication.

- Each communication between customer and service provider takes place confidentially, i.e. it is encrypted.
- If an error occurs during the course of a protocol by a protocol participant, then he informs the other protocol participant and then terminates the protocol.

In the following, the principle of the protocols of the *IBM idemix* anonymous credential system is described in order to subsequently identify its security properties for use in business processes.

Issue and Verification of an Anonymous Credential

The issue of an anonymous credential for a customer and its authentication with an anonymous credential takes place in four steps, whose course is shown in Figure 5.18. In the first step, customer U establishes a connection with the certification authority CA and agrees with it on a pseudonym(U,CA). If the customer is authorised to receive the requested credential to the data attributes, then the CA issues this credential by digitally signing the relation between the data attributes and the customer or his pseudonym(U,CA). The certification authority subsequently sends the resultant credential credential(attributes, pseudonym(U,CA),CA) to the customer U. The customer U can now identify himself with this credential towards the service provider SP. He previously agrees on a further pseudonym pseudonym(U,SP) with the service provider SP. The generation of this pseudonym is necessary to be able to verify the relationship between the pseudonym pseudonym(U,SP) and the credential credential(attributes, pseudonym(U,CA),CA). For this, a test value was calculated with the issue of credential for the pseudonym pseudonym(U,CA), which is again used for a credential verification and shows the relationship to the pseudonym pseudonym(U,SP). Verification of the credential takes place in the fourth step through a zero-knowledge proof. Customer U proves to the service provider SP that he is in possession of a valid credential credential(attributes,pseudonym(U,CA),CA), without disclosing the data of the credential and the secret symmetric key k_U. In concrete terms, customer U proves the following:

- He is in possession of a digital signature of the certification authority CA that refers to the maintained data or attributes of a customer with the pseudonym pseudonym(U,SP).
- He knows the secret key k_U on which the pseudonyms pseudonym(U,CA) and pseudonym(U,SP) are based.

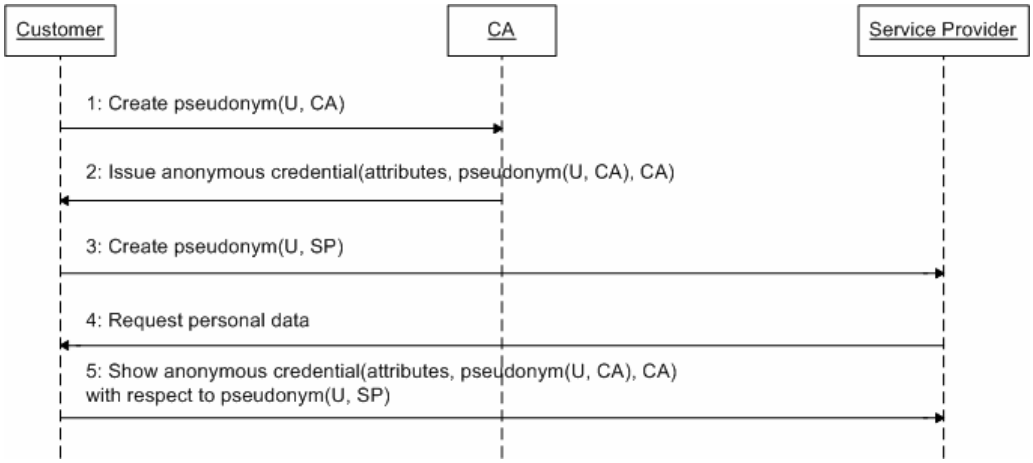

Figure 5.18 Sequence of an issue and usage of anonymous credential in the *IBM idemix* basic system.

The customer does not send the anonymous credential in plain text for verification but a cryptographic commitment (Brassard, Chaum and Crépeau, 1988). The confidentiality of the credential data is therefore ensured with a verified linking of this data to the assertion to be proven of the anonymous credentials. Together with the use of zero-knowledge proofs, *IBM idemix* prevents several verifications of the same credential being able to be linked together and with the issue of this credential of service providers and certification authorities. This is also the case when all service providers and certification authorities pool their profiles over all transactions. The customer is therefore only known to the service providers for the verification of a credential by the used pseudonym and the proven assertion of the credential. If the customer uses a new pseudonym for each transaction, then, under the previously specified assumptions, he is anonymous.

5.3.4.2 Extensions of Anonymous Credentials in the *IBM idemix* System

Based of the presented basis system, *IBM idemix* supports a disclosure of selected personal data or their attributes, anonymous one-show credentials that are precisely valid for a one-show verification, the revocation of the pseudonymity or anonymity of the customer under certain conditions and the revocation of anonymous credentials.

Verification of Selected Personal Data

A customer can determine himself which data of a credential is disclosed for the authentication with a credential towards a service provider. The disclosure of a certain assertion is also possible for him depending on the attested date. If a credential is, for example, a confirmation of the date of birth and the current age of the customer, e.g. date of birth = 19.02.1973 and age = 33, then the customer can decide whether he wishes to prove the assertion of age > 21.

Anonymous One-Show Credentials

IBM idemix supports the use of anonymous one-show credentials. An anonymous one-show credential is only valid for precisely one verification. If an anonymous one-show credential is used for the second time, this multiple use can be detected. For the detection of a multiple usage, IBM idemix uses an off-line test analogous to the tests for electronic coins (Chaum,

Fiat and Naor, 1990), i.e. there is no communication between the service provider and the issuing certification authority on the verification of a multiple issuance. If a one-show credential is used for the second time, this results implicitly in a protocol note with which a de-anonymisation provider can disclose the pseudonym of the customer or the issue of this credential or his identity. A multiple usage is thus not prevented but subsequently detected and the customer concerned can be identified.

Revoking Anonymity of a Customer in Case of Fraud

IBM idemix supports two mechanisms for revoking anonymity. Either the identity of a customer or his pseudonym he used for the issue of a credential can therefore be disclosed. The first case concerns all the customer's transactions and reaches their accountability to the identity of the customer. It involves a global de-anonymisation. The second case refers to the use of a certain credential and the related transactions where this credential was used. Revoking the anonymity is locally related to these transactions.

Revoking a customer's anonymity requires a further service provider, namely a de-anonymisation service provider DA. In order that the anonymity of customer U can be locally detected, the protocol on the verification of a credential credential(attributes, pseudonym(U,CA),CA) is changed as follows (see Figure 5.19): Customer U encrypts his pseudonym pseudonym(U,CA), which he has used for the issue of the credential, with the public key pk_{DA} of the de-anonymisation service provider DA. This encryption is verifiable, i.e. the service provider SP receives proof through the encryption that the de-anonymisation service provider can decrypt and disclose encrypted pseudonym pseudonym(U,CA) with the notes of the protocol sequence between the customer U and the service provider SP.

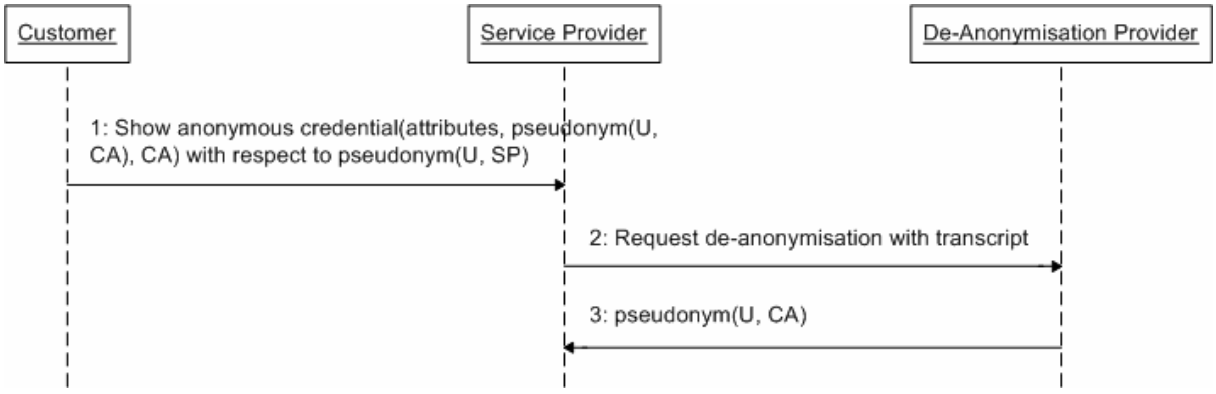

Figure 5.19 Basic sequence of revoking customer's anonymity.

Before the verification of an anonymous credential, customer U and the respective service provider agree on the conditions under which his anonymity is going to be disclosed. Should the anonymity be revoked, the respective service provider sends this agreement together with his notes of the protocol sequence to the de-anonymisation provider. The latter can decide on the basis of the protocol notes whether the conditions agreed between the customer and the service provider have been observed. If this is not the case, then the de-anonymisation provider reveals the pseudonym pseudonym(U,CA) of the customer and sends it to the service provider.

The global revocation of anonymity uses the same protocol variants. The *idemix-PKI* is extended by a certification authority that only issues credentials for a pseudonym for a person if it knows his identity. This certification authority for identities thus issues a type of digital personal identity card with an anonymous credential. The customer can also use this anonymous credential under various pseudonyms in order to receive further anonymous credentials.

Revoking an Anonymous Credential

The revocation of an anonymous credential takes place in the *idemix-PKI* through the certification authority that issued this credential (Kohlweiss, 2003). Dynamic accumulators are used for the revocation of anonymous credentials (Camenisch and Lysyanskaya, 2002). A dynamic accumulator is a value that is sequentially calculated by all non-revoked anonymous credentials. The respective prime number e(U,CA) (Camenisch and Lysyanskaya, 2001) is used representative of the anonymous credential as exponent for the calculation of the accumulator according to the RSA procedure [Riv1978]. For the verification that an anonymous credential was not revoked and therefore entered into the calculation of the related accumulator, a witness value (witness) is used. A dynamic accumulator and the operations of add and delete are specified in (Camenisch and Lysyanskaya, 2002).

5.3.4.3 Applying *IBM idemix* on Multi-Stage Business Processes

Since all anonymous credentials and pseudonyms of customer are based on his secret key k_U, a delegation of anonymous credentials also implicitly means the transmission of k_U. The transmission of anonymous credentials is explicitly not supported by *IBM idemix*. Two mechanisms are in fact used which should prevent a delegation of credentials. This involves a PKI-based and an all-or-nothing non-transferability of credentials (Camenisch and Lysyanskaya, 2001).

For a PKI-based non-transferability, the customer's secret key k_U is linked to his private key sk_U. For this, a certification authority outside the *idemix-PKI* certifies the external public key of customer U. Furthermore, the customer deposits the pertaining private key sk_U in encrypted form with the certification authority which then publishes it. This encryption is made with the symmetric key k_U. If the customer transmits his secret key k_U, he also transmits with it his private key sk_U. Each person in possession of the symmetric key k_U can encrypt the private key sk_U of customer U.

With all-or-nothing non-transferability of anonymous credentials, all credentials and pseudonyms of a customer in an *idemix-PKI* are transmitted if the customer transmits his secret key k_U. The all-or-nothing non-transferability of credentials is based on the use of the secret key k_U for each generation of a pseudonym and publication of all pseudonyms, credentials and the pertaining test values. In order to use these, only the information about the secret key k_U is missing. If customer U transmits it, his proxy can use all the customer's pseudonyms and credentials without restrictions.

Figure 5.20 shows the use of *IBM idemix* for a business process with a proxy. Steps one to four proceed analogously to the use of *IBM idemix* in a single-stage business process. In step five, however, must the customer transmit his secret key k_U with the requested data, in the form of an anonymous credential, to his proxy so that he can use this anonymous credential in the eighth step where the target service provider is concerned. The transmission of the secret key k_U is based on the all-or-nothing non-transferability attribute of the *IBM idemix* system.

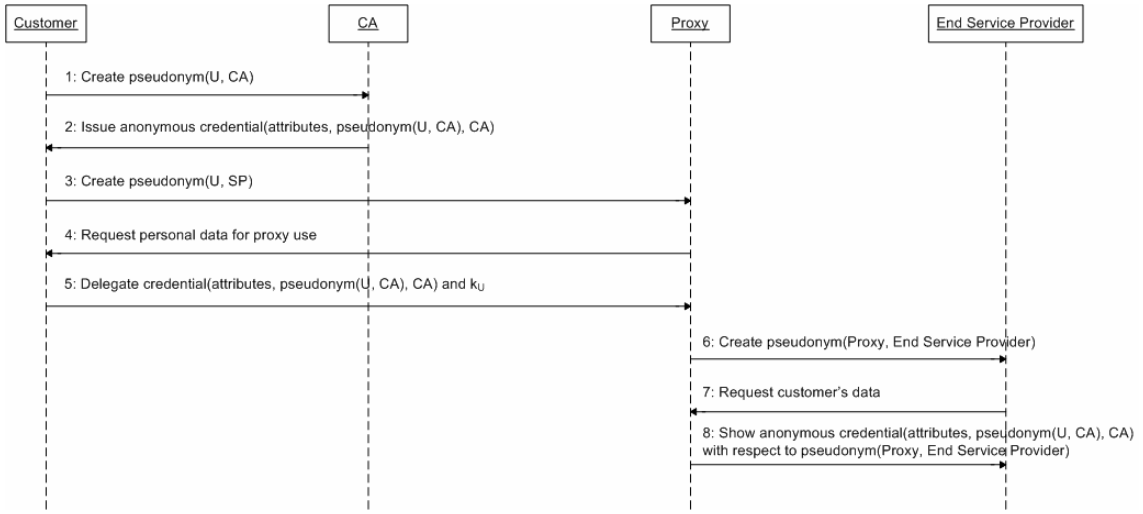

Figure 5.20 Use of *IBM idemix* on multi-stage business processes with the use of the all-or-nothing non-transferability of anonymous credentials.

5.3.4.4 Security Properties of *IBM idemix*

IBM idemix is primarily an anonymous credential system that is in fact integrated into an identity management system (Camenisch, Shelat, Sommer, Fischer-Hübner, Hansen, Krasemann, Lacoste, Leenes and Tseng, 2005). Since *IBM idemix* is independent of an identity management system though, the security properties of the credential system are analyzed in the following. A secure data storage and a situation-dependent release of personal data are not part of the system but can be extended by an identity management system. The security properties of *IBM idemix* for access to personal data are as follows:

- **Unlinkability of transactions:** Through the use of pseudonyms and of the attribute of zero-knowledge proofs used for the verification of anonymous credentials, various transactions of a customer U cannot be traced back to him without further information.
- **Authentication without showing identifying data:** The *IBM idemix* anonymous credential system uses zero-knowledge proofs with the issuance and verification of anonymous credentials and pseudonyms. The connection between the credential and pseudonyms to the secret key k_U of customer U remains concealed, but without giving up the accountability of his transactions to him. This anonymous can be extended to the certified personal data of a customer, so that its attribute but not the concrete value is verified with an authentication. This results in no identifying data about customer U accruing during his authentication and an undesirable identifying and profile formation is therefore avoided.
- **Non-repudiation of customer's transactions:** Through the linking of anonymous credentials and pseudonyms to the secret key k_U of the customer and its application in the protocols of *IBM idemix*, an accountability of the transactions to the owner of k_U, i.e. the customer is guaranteed.
- **Revoking customer's anonymity in case of fraud:** The extension of the basis system by a de-anonymisation provider achieves the lifting of a customer's anonymity in the case of fraud. However, he either only discloses the anonymity

for transactions on a certain anonymous credential or all transactions on all the anonymous credentials of a customer. Without additional information, i.e. the protocol notes, a lifting is not possible. The customer must in fact trust the de-anonymisation provider that he only discloses the customer's anonymity in the case of a verifiable breach on his part of the agreed conditions.

A controlled usage of personal data is not considered by *IBM idemix*. Both mechanisms for non-transferability of anonymous credentials in fact prevent a delegation. If *IBM idemix* is used for the transmission of personal data in the form of an anonymous credential to a proxy, however, the customer will lose the control over the usage of all of his certified data and pseudonyms.

5.3.4.5 Conclusion

With the *IBM idemix* anonymous credential system, a customer can use services anonymously and at the same time verify certain attributes or data of his person with anonymous credentials. No identifying data about the customer is known with the authentication with an anonymous credential, provided that service does not require it. On the other hand, his anonymity can be revoked by a certain service provider and under previously agreed conditions. This service provider cannot however relate all the customer's transactions if the revocation of the anonymity only applies to a certain anonymous credential.

IBM idemix therefore fulfils the criteria for the protection of privacy concerning access to personal data with the exception of secure storage of data and the situation-dependent release of personal. These criteria are not considered by *IBM idemix*. Privacy is however not protected with regard to the use of transmitted personal data. The protocol specification of *IBM idemix* in fact provides two mechanisms which should prevent a delegation of anonymous credentials and with the use on multi-stage business processes result in a loss of control of the customer over his identity. According to these assumptions, the customer must trust his proxy when using *IBM idemix* as with the delegation of the secret key k_U the customer delegates his identity or the amount of his credentials and pseudonyms and his proxy can use these without restriction.

5.4 Security Requirements for Identity Management in Business Processes

The analysis on a customer's privacy and on security interests of the service providers involved shows the focus on the protection goals of confidentiality with regard to the personal data of the customer and accountability with regard to the transactions of the data provider, whether he is a customer or his proxy. In summary, the analysis shows that a customer's privacy is violated precisely when his consent for data collection, processing, storage and delegation is contravened. With his consent, a customer provides the framework in which the respective personal data can be processed. This framework also contains the particulars of the parties, i.e. the service providers who should have access to the data and can use it according to the consent. Thus, an authorisation for the service providers concerned for processing the specified personal is on hand with a customer's consent. Moreover, it must be ensured that unauthorised persons are refused access to the customer's data and his communication relations in order to avoid abuse and profile creation. Based on the identified threats, the requirements of such an access and usage control system for identity management are

described in the following. The requirements refer to the access to personal data in the first part and to their application in the second part.

5.4.1 Access to Personal Data

In order to self-determine the disclosure of personal data by a customer, identity management systems have the following properties concerning access to personal data:

- **Secure data storage:** According to assumption, a customer governs his data with a personal end device. In order that unauthorised persons do not gain access to his data it must be confidentially stored on the end device.
- **Situation-dependent disclosure of personal data:** To counteract an undesirable creation of profiles and a collection of identifying data, the customer is able to control the release of his personal data. The situation, i.e. the respective service provider and the desired service, is to be thereby taken into consideration (Jendricke, 2002). In addition to a conscious release of his data, it is also possible for a customer to have profiles generated in such a way that they do not overlap and that these various transactions of the customer cannot be traced back to him. However, this is only the case when two applications require different customer data for their service.
- **Delegation of the minimal authorisation:** If an authorisation is to be used for access to a customer's personal data, then the access is only concern the minimal customer data required for the purpose of data economy according to the *Least Privilege* principle (Saltzer and Schroeder, 1975). The requesting service provider should not receive additional data with such a specified authorisation. This property concerns the release of personal data if it is externally governed by a service provider. This corresponds to the access to a profile generated about the customer and, depending on the scope of the authorisation, enables a linking of profiles.
- **Unlinkability of transactions:** If a customer appears under various pseudonyms, he can protect himself from a linking of his transactions and the profiles thereby generated. Depending on the type of pseudonym, the protection goal of accountability is at the same time fulfilled. This takes place subject to the number of persons appearing under the same pseudonym. If a customer only uses transaction pseudonyms, i.e. for each transaction a new pseudonym different from the previously used pseudonym is used, then each transaction appears uniquely. For a differentiation of pseudonym types and the associated possibility of a clear identification of a person, reference should be made to the classification of Andreas Pfitzmann und Marit Hansen (Pfitzmann and Hansen, 2006).
- **Authentication without showing identifying data:** In order to protect himself from undesirable identification and linking of transactions, a customer is able to authenticate himself towards a service provider but without showing identifying data. One example is the proof of nationality by the customer verifying that the respective identity card was issued for him but without revealing its data, e.g. the personal identity card number.
- **Non-repudiation of customer's transactions:** Identity management systems guarantee that a transaction is clearly related to the agent, i.e. the customer or his

proxy. Even if a pseudonym appears with a transaction, it cannot be used by the recipient of the pseudonym without further measures. This rules out an abuse of the transmitted data, i.e. the partial identity with the pseudonym.

- **Revoking customer's anonymity in case of fraud:** In order that prosecution is possible in the event of fraud and the fraudster can be called to account, his identity can be revealed. A case of fraud is to be clearly related to the fraudster together with the non-repudiation requirement of transactions.

These properties apply to the disclosure of personal and identifying data. At the same time, the security interests of the service providers can be preserved. These properties are however inadequate if personal and identifying data of the customer is needed for a service by another service provider. In the following section, the security requirements for controlling the use of personal data by identity management are derived from the threats of abuse and a delegation of customer data.

5.4.2 Use of Personal Data

The security requirements of usage control are aimed against an abuse and undesirable delegation of collected customer data. At the centre of the security requirements for a use determined by the customer of his collected data is his consent in the form of an authorisation. An authorisation contains the rules for the access to and the use of the customer's personal data. The security requirements for usage control are as follows:

- **Reference to purpose of an authorisation:** If an authorisation is used for the use of personal data, then is should specify the connected purpose of collection and the subsequent processing, duration of storage and assertions for delegation of this data. The rules of the authorisation apply to the customer data concerned, the service provider who is hereby authorised for the usage, the operations to the customer data and to the period of time during which the usage is permitted.
- **Restricted delegation of an authorisation:** If a service provider delegates a received customer authorisation to further service providers, the authorisation should only be valid if the customer has agreed to the re-delegation and a further authorisation relating to this is on hand.
- **Revocation of an authorisation:** A customer should be able to revoke an authorisation for a proxy at any time if a proxy has turned out to be an attacker, the purpose of the data use has been prematurely completed and the original customer data is no longer up-to-date or invalid.
- **Integrity of an authorisation:** A modification of an authorisation should be detected in order to prevent an abuse after receipt of a correct authorisation and to prevent or retrace it.
- **Enforceability of an authorisation:** An authorisation should be able to be enforced according to its rules and limits so that an abuse of the pertaining customer data and its delegation by a service provider are ruled out. If it is not possible to enforce an authorisation, then the use of the associated customer data according to the authorisation should be traceable.

- **Access to collected personal data:** Customers should have access to automatically generated profiles that may be applied to them and the possibility to actively adapt their own profiles.

Together with the requirements of an access to personal data, an access and usage control mechanism therefore ensues with which a customer can protect his privacy in the sense of informational self-determination in single or multi-stage business processes.

5.5 Case Study: Using Attributes as Access Rights in eGovernment

We now present **private** solutions to two key problems facing many governments: identification cards and traffic regulation. Both of our solutions work with an offline authority.

First, consider an example. Suppose Alice wants to use her government issued driver's license to convince a bar owner that she is over the age of 18. In the common non-private solution (which is currently the de facto standard), Alice provides her complete driver's license to the bar owner, which includes her name, birth date, address, and other personal information. The bar owner uses the birth date to confirm that Alice is over 18. A benefit of this solution is that it is both fast and simple. However, once Alice's digital credentials are scanned by a computer, rather than simply looked at by a human, Alice's personal information may be easily exploited (e.g., unsolicited mail sent to her address) or used to track her personal habits (e.g., the bar might keep a detailed record of when she came in and who else came in shortly before or after her.)

In a private solution, Alice and the bar owner could instead execute a protocol, at the end of which the bar owner will be convinced that Alice has a valid driver's license with a birth date making her over the age of 18 but will learn nothing else about Alice (including her name and actual birth date). Such systems are called anonymous credential systems (e.g. (Camenisch and Lysyanskaya, 2002)). They use cryptographic techniques to selectively reveal portions of a credential, as chosen by the user. A benefit of this solution is that is it very privacy friendly. Although, its implementation is more involved than the standard solution, the underlying cryptographic protocols are reasonably efficient.

When we talk about e-Government, two primary use cases come to mind: identification cards and road tolls. Let us briefly discuss both scenarios.

5.5.1 Identification Cards

IBM idemix (identity mixer) is an anonymous credential system developed by IBM which is currently being extended to support the guidelines for machine readable travel documents [Int06] that were put forward by the International Civil Aviation Organisation.

With an *idemix* credential, a user can either hand over all of her personal information (as is currently done today) or can selectively release information by proving statements of the following form:

- The user is between the ages of X and Y (without revealing her actual age).
- The user belongs to a certain group (without revealing which group member she is). For example, a user in the USA might prove that she is from an East Coast state without revealing which one.

- The user does not belong to a certain group (without revealing any additional information). For example, a user might prove that her blood type is not A-negative.

5.5.2 Road Tolls and Intelligent Cards

Most major cities world-wide are experiencing alarming levels of traffic congestion and accidents. To mitigate congestion, many cities (such as London) are charging a toll each time a vehicle enters or exits the city. To mitigate accidents, transportation officers are designing intelligent cars that report their locations to the road infrastructure and to each other to help the human driver avoid accidents. Governments implementing these systems again have to make privacy-impacting choices.

Consider the case of intelligent cars. Bob might attack the system by flooding the infrastructure with reports of traffic congestion on any road that he is on. This way, the infrastructure tells nearby cars to avoid Bob's route and he enjoys a quick drive to work. This problem can be avoided by making Bob's car digitally sign all reports it issues and accepting only one report from Bob each minute. Unfortunately, this solution creates a privacy problem, because now Bob's driving patterns can be easily monitored by the government.

Recently, (Camenisch, Hohenberger, Kohlweiss, Lysyanskaya and Meyerovisch, 2006) proposed an efficient k-anonymous authentication system, where a user, call him Bob, can anonymously, but authentically issue up to k reports per an arbitrary time period. If Bob maliciously tries to issue k +1 reports, this cheating will be detected, Bob's identity will be revealed, and he can be punished accordingly. If Bob acts honestly, however, the government will not be able to link his anonymous reports.

5.6 Conclusion

Identity management as the current security mechanism to preserve privacy is used to realise the principle of data economy. But, as chapter four shows, personalised services need personal data of their customers. As nowadays, there is no security mechanism for privacy, when personal data are disclosed. Customers have to trust the corresponding service providers. Implementing privacy-aware business processes lacks of an overview of collected customers' data, the use of these data in business processes and whether a customer has given consent to processing his data for the given purpose. The contribution of the IBM Enterprise Privacy Architecture is a process model for service providers to model their business processes according to data protection directives and laws and to use an internal access control with audit functionality to ensure a compliant use of customers' data within a service. In order to implement the derived process model for data protection, section 5.2 suggests the approach of security process models. But furthermore, customers have to trust their service providers to whom they have disclosed personal data. They are not able to determine or control the use of their data.

As this chapter shows identity management is, as an access control mechanism on personal data, a countermeasure for undesired collection of personal data, identification, profiling, and linkability of transaction as long as it is used in single-stage business processes. But identity management systems lead to "Big Brother" and abuses by undesired impersonation, if they are applied in business processes with proxies. Even the only identity management system (*Liberty Alliance*) considering multi-stage business processes has a contradiction in its trust model with respect to privacy: untrustworthy service providers become imperatively

trustworthy service providers for the customer. Consequently, there is a need for a usage control mechanism as an extension for identity management in order to preserve privacy by an access control on personal data for controlling the disclosure of them at the same time by an usage control in order to control or verify the use of disclosed personal data with respect to customer's privacy policy. The next chapter describes such an extension for identity management by protocols for an unlinkable delegation of rights as authorisations for the use of disclosed personal data. In ambient intelligence environments, e.g. sensor networks, customers are not aware of a data collection. So that customers are able to retrace the disclosure of their profiles in order to identify service providers which have abused or re-delegated customers' data without their consent, a history mechanism for the disclosure of personal data is introduced: 'Data Track'.

6 Approaches for Identity Management Extensions for Business Processes

This section presents two extensions for identity management concerning the use of disclosed personal data and the ability for customers to retrace the collection of their profiles. Section 6.1 introduces the usage control mechanism *DREISAM* together with its application on the case study *loyalty program*. Section 6.2 the history instrument for customers *Data Track* in order to retrace data collection. Section 6.3 concludes this chapter.

6.1 Unlinkable Delegation of Rights by DREISAM

If a customer uses personalised services in a single-stage business process, the threat to his privacy exists in the undesirable linking of his individual profiles. He can protect himself with identity management through a controlled release of personal data, so that his profiles appear independent of each other. However, this has so far not been technically possible with personalised services in a multi-stage business process. The *DREISAM* delegation system presented in the following is a usage control mechanism, with which a customer-controlled disclosure of personal data is now also achieved in multi-stage service processes. A customer must not transmit his secret authentication token, e.g. his secret cryptographic key k_U, but an authorisation for the use of certain personal data or partial identities for a predetermined purpose. The added value of *DREISAM* is that a customer can be unlinkable for several delegations and thus over several transactions. A linking of the profiles resulting in each case on this customer is thereby hindered in that, at best, no identifying data accumulates in more than one profile. *DREISAM* extends current identity management systems.

DREISAM specifies a credential-based usage control mechanism for a delegation and use of personal data to a proxy. Through the agreed privacy policy, this usage control defines the framework in which disclosed personal data can be used by a proxy. A customer can control the disclosure of personal data, also via a proxy, through the use of anonymous credentials and thus protect himself from an undesirable combination of his profiles.

Section 6.1.1 presents the usage control model on which *DREISAM* is based. The protocol for a delegation of an authorisation for the use of personal data is specified in section 6.1.3. Section 6.1.4 focuses to the same degree on the revocation of a delegated authorisation.

6.1.1 Model of Usage Control for Privacy in Multi-stage Business Processes

Multi-stage business processes are characterized by a proxy of a customer having to obtain the customer's personal data so that he can make use of subsequent services in the interests of his customer. Personal data of a customer is, on the one hand, the object of access and, on the other, an authorisation for the proxy to obtain access to services of a further service provider. There are several options for a customer to delegate personal data and with it the receipt of a relevant anonymous credential for a proxy. He can either delegate his secret authentication token for anonymous credentials, i.e. his secret key k_U, issue an anonymous credential with the relevant data himself for his proxy, or have it issued by a certification authority.

The transmission of the secret key k_U does not present a possibility due to the resultant loss of control of the customer over his identity. The second possibility also does not come into consideration. If a customer were to issue an anonymous credential for his proxy, then the

customer is firstly identifiable by way of the digital signature of the credential and, secondly, these credentials must be accepted by the end service provider. The third possibility is therefore selected: a certification authority issues anonymous credentials for the personal data to be delegated and their attributes on behalf of the customer to his proxy. In addition, the customer sends an authorisation for the use of the personal data required to his proxy.

An authorisation applies to a certain amount of personal data, i.e. to a partial identity and not to the whole identity of the customer. With the delegation of an authorisation, a proxy is authorised to receive the specified partial identity of the customer and use it for a certain purpose. The purpose of use is defined by the conditions of an authorisation. As a countermove, a proxy is committed with regard to the handling of the partial identity received. The decision about the release of a partial identity to the proxy is made by the data provider managing the partial identities. Since personal data is used in the form of a credential and the proxy will therefore receive a credential on the partial identity, this decision is made by a certification authority. This involves the certification authority which will issue the credential for the proxy.

Whereas user-centric identity management to date is an access control mechanism for personal data and authorisations apply to the access to data, it is now by *DREISAM* possible to additionally apply it to the use of delegated data. The model is thereby expanding from access control to usage control. A general model for usage control was first defined by Park and Sandhu (Park and Sandhu, 2004). They extend the access control model with the components of *obligations* and *conditions* and thereby present decision factors for the use of systems and data, generally by objects. An obligation corresponds to a commitment by means of which it is examined whether obligatory requirements are fulfilled before or during a usage decision. Conditions, on the other hand, take into account environmental or system attributes such as the time or CPU-ID. The usage control model for the privacy in accordance with informational self-determination consists of two parts: the disclosure of personal data is specified by an access control model and the use of the disclosed data by a model of usage control.

The parties involved in the access control model are the customer, his proxy and a certification authority. Through a confirmation, a certification authority regulates the access to personal data by attesting the relationship between the data and a proxy for disclosure. Figure 6.1 shows these relationships.

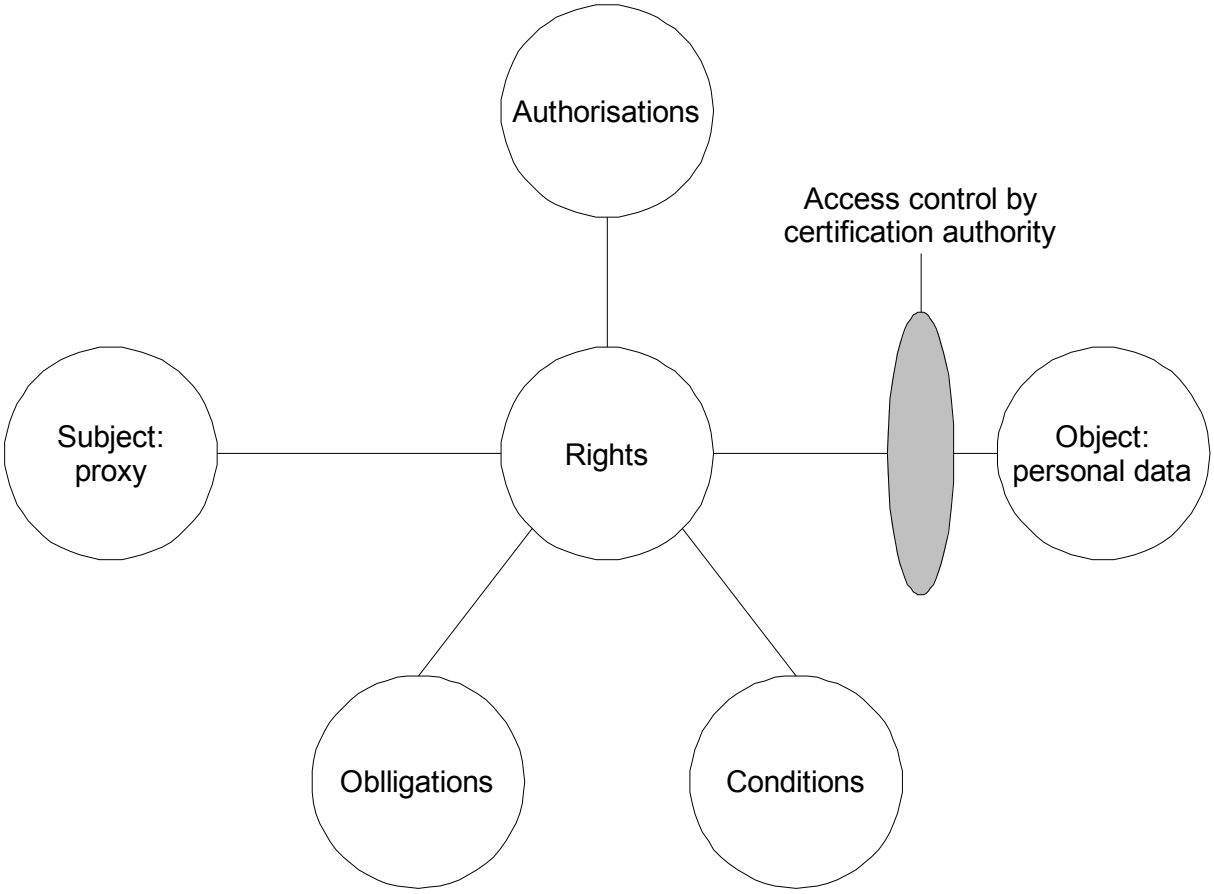

Figure 6.1 Access control model for a disclosure of personal data.

As soon as the personal data requested is delegated to a proxy and he wants to use it as far as a further service provider is concerned, the data no longer constitutes the object of access but an authorisation for access to the further service. The usage control model from Figure 6.2 now applies to the security interests of the requested service provider. The conditions remain preserved in their role, however, due to their independency of subject and object of access, provided that there is no conflict with the interests of the service provider. The obligations are again directed towards a proxy, but are now called for by the requested service provider. Instead of a certification authority, the respective end service provider now takes over the usage control and thereby enforces its security interests.

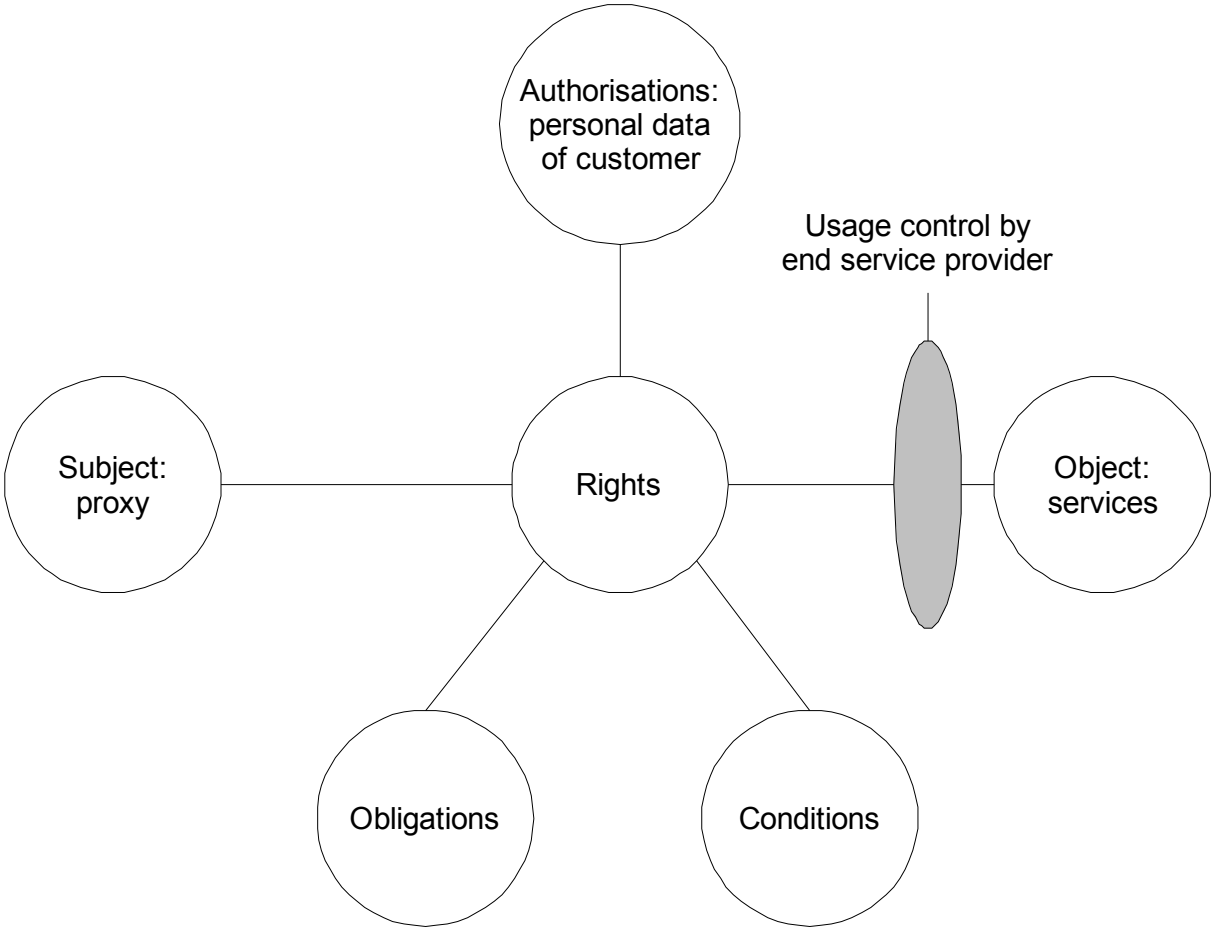

Figure 6.2 Model of the usage control for the use of personal data by a proxy.

6.1.1.1 Access and Usage Rights in the Form of a Privacy Policy

The usage control of a customer's personal data is regulated by his security interests. A customer defines his interests as rules in the form of a privacy policy. A rule applies to the data concerned, its recipient and the permitted ways of processing, i.e. to the purpose of a service process. The use of the data involved applies to the service provider, with whom a customer directly communicates and who assumes the role of a proxy in the case of a multi-stage service.

The proxy role is the central focus of the privacy policy. According to the terminology of usage control (Park and Sandhu, 2004), the subject is a service provider or proxy, the object is the requested personal data or its assertions and the types of rights then result from the assigned authorisations, conditions and obligations. A privacy policy together with an authorisation presents the relationship and defines the use of personal data as follows:

- **Proxy:** The personal data released or its statement may only be delegated to the service providers specified here in their role as proxy. For this, the customer specifies a list of his proxies as subjects.
- **End service providers:** A proxy may only release the personal data transmitted to him to certain types of services or service providers. The limitation is specified by a list of the recipients.

- **Number of permitted usages of personal data:** If the frequency of the use of personal data is known to the customer before a delegation and he does not wish to agree to unrestricted utilization, then he restricts the number of uses by an upper limit.
- **Re-delegation:** At this point, the customer specifies whether his proxy may re-delegate the delegated authorisations and the pertaining data.
- **Validity:** An authorisation for the personal data delegated by a customer is only valid for a certain period of time. The period of time is defined with a commencement and termination date.

The enforcement of a privacy policy depends on the interest of the service providers and the certification authority. In order for an enforceable privacy policy to ensue, interest conflicts between the parties must be detected and, if necessary, compromises be negotiated. The resultant authorisations should then no longer be able to be altered. In the following, the demands on authorisations and their realization is addressed.

6.1.1.2 Authorisation in the Form of a Proxy Credential

The following demands on an authorisation are derived from the privacy threats according to the threat analysis from chapter five:

- **Purpose-related use of an authorisation:** A delegated authorisation should only be valid for the purpose of the service, i.e. it is linked to the identity of the proxy and that of the subsequent service provider, the required function call of his service or its type and the number of usages permitted for a specified time.
- **Restricted delegation of an authorisation:** If a proxy relays his authorisation, it should only be valid if the customer has agreed to this transmission.
- **Revocation of an authorisation:** A customer should be able to revoke an authorisation for a proxy at any time, if a proxy has turned out to be an attacker, the delegated task has been completed earlier than expected or the customer's credential concerned has expired or been revoked.
- **Integrity of an authorisation:** Assuming that an attacker cannot break a cryptographic primitive, an alteration of an authorisation should be able to be detected.
- **Delegation of the minimal authorisation:** A delegated authorisation for the proxy should apply exclusively to the disclosure of the customer's data that is necessary for the proxy's task.
- **Enforceability of an authorisation:** The access control decisions of a certification authority and usage control decisions of an end service provider should follow the restrictions of a delegated authorisation. Either a customer has to control these decisions or they should be verifiable by the customer afterwards.

The first requirement applies to the service provider and in his service as proxy. This is fulfilled by the public key specifications pk_{Proxy} of the proxy as his unique identifier, the unique transaction number TID of the pertaining service process, a timestamp of issuance and the validity time period with commencement and termination date. The customer has received the key pk_{Proxy} with the authentication of the proxy. Information about the delegation of an

authorisation is recorded as a further attribute in the proxy credential. Furthermore, a proxy credential is clearly identified by a serial number. This is necessary, for instance, in the event of a revocation of an authorisation. The fourth requirement is fulfilled by an authorisation being realised as an attribute certificate (Farrell and Housley, 2002). Through the digital signature of a certificate, its contents are protected against a modification. An attribute certificate as authorisation is specified in the following as a *proxy credential*. The fifth requirement is fulfilled by the specification of the data to be delegated or the partial identity of the customer in a proxy credential. A revocation is made through a protocol.

In order that no profile can be made about the customer by means of his proxy credentials, they are issued by a certification authority. If a customer should otherwise issue proxy credentials, he digitally signs them with his private key sk_U and can consequently be linked by way of his digital signature or its verification with the corresponding public key pk_U. A certification authority, on the other hand, replaces the customer in the certification paths for the verification of a proxy credential. From the end service providers' viewpoint, a certification authority examines on their behalf whether the personal data or the specified attributes pertain to this customer and whether he is authorised to delegate it. A proxy credential is similar to a Kerberos V5 ticket-granting ticket (Kohl and Neuman, 1993). However, it does not contain any revealing data about the identity of the customer.

6.1.1.3 Execution of Usage Control

The execution of usage control applies both to a disclosure of personal data as well as to its use. As a disclosure is done by anonymous credentials, which are issued by a certification authority, this executes customer deciding with the attestation for a delegation of personal data. Once the data is disclosed, neither a customer nor a certification authority has the possibility to control the use of this data. Disclosed data could therefore be used by a proxy for other purposes as often as desired.

In order that data is not delegated at will and its unrestricted use is detected, a certification authority delegates requested data of the customer only after submission of a valid proxy credential and in the form of an anonymous one-show credential to the authorised service provider. The incentive for a proxy not to use an anonymous one-show credential several times lies in the integration of a secret of the proxy in such a credential and its publication in the event of multiple usages (Camenisch and Lysyanskaya, 2001). For this purpose, *DREISAM* encodes the secret cryptographic key k_{Proxy} of the proxy into an anonymous one-show credential. An end service provider detects a multiple usage of an anonymous one-show credential and should reject the proxy's associated access enquiry. It can also come to unlimited usage if a proxy receives an anonymous one-show credential for each application. A certification authority therefore logs its issuance of anonymous one-show credentials.

In addition to $k_{Proxy,}$ restrictions for use are integrated into an anonymous one-show credential that corresponds to the rules of the customer on the use of delegated personal data. The restrictions apply to the validity of the credential, the service providers allowed and the naming of the service functions permitted as well as the specification as to whether the personal data can be transmitted.

The verification of a delegation of personal data and the logging of the delegation is carried out by means of a list. This list, which is referred to in the following as a delegation list, is similar to the presentation of an access control matrix according to (Harrison, Ruzzo and

Ullmann, 1976). The relationship between the access object, the object of protection and the type of rights certainly forms the basis for an access decision. However, these three objects are not firmly specified in the case of the delegation of personal data. They are determined by the customer for each delegation in his delegation application through his privacy policy and the personal data concerned. In addition, an entry of a delegation list refers to the transaction of the customer with his proxy and to the owner of the data to be transmitted, i.e. the customer. In order that a certification authority can solve a dispute between customers and service providers concerning a delegation, the pertinent credential of the customer is stored in an entry. For monitoring the frequency of the data transmitted to a proxy, the number of the transmissions involved for each delegation is recorded. An entry of a delegation list comprises the following attributes:

- a unique transaction identifier (TID),
- the pseudonym pseudonym(U,CA) of the customer, under which he is known to the certification authority,
- his personal data to be transmitted or its attributes,
- his anonymous credential credential(attributes, pseudonym(U,CA),CA),
- his privacy policy for the transmission and use of personal data,
- the name of the proxies who have already received anonymous one-show credentials for this data
- for each proxy, the number of the anonymous one-show credentials issued.

6.1.2 Phases of a Delegation and a Revocation of an Authorisation

The combination of access control with usage control forms the model for the *DREISAM* delegation mechanism. This section introduces the model and the *DREISAM* protocols in detail.

6.1.2.1 Participants and Assumptions

The customer, as owner of his data, his proxy, a certification authority and a (end) service provider participate in the protocols of a delegation of an authorisation and its revocation. The revocation of a customer's anonymity or that of his proxy takes place unchanged according to the protocol from (Camenisch and Lysyanskaya, 2001) and therefore requires a de-anonymisation party.

It is assumed that there is a PKI for anonymous credentials according to (Camenisch and Van Herreweghen, 2002). The customer trusts the certification authority involved that it examines the relationship of attributes to a person according to its certification policy and thereupon issues credentials. The communication of the customer with the service providers is unobservable as far as third parties are concerned through the employment of anonymity services. It is furthermore assumed that the communication partners mutually authenticate themselves before a communication. Should a participant in the protocol detect an error in the protocol sequence, he will immediately inform his communication partner and terminate the protocol sequence. It is moreover assumed that the personal data to be delegated has already been attested by a certification authority and the customer has the respective anonymous credential according to (Camenisch and Lysyanskaya, 2001).

6.1.2.2 Phases of the Delegation of an Authorisation

A delegation of an authorisation for the use of personal data or its attributes and their application is carried out in four phases with *DREISAM*. Phase A considers the application of a proxy for personal data from the customer. Phases B and C implement the usage control for a disclosure and use of personal data, whereby a certification authority regulates access to the customer data received. The aim of phase B is the issue and delegation of an authorisation for a proxy, so that he can use the respective customer data and prove its authenticity without knowledge of the secret key k_U. Phase C aims at the transmission of the requested customer data to his proxy. In this phase, the decision to disclose the data concerned is made by the certification authority depending on the authorisation of the proxy. Since the protocol runs within the framework of a PKI with anonymous credentials, the data, in the form of an anonymous one-show credential with its conditions for use stemming from the customer's privacy policy, will be linked to the proxy in the event of a positive decision. With Phase D, a delegation is concluded. This phase aims at the purpose-related use of delegated data according to the security regulations of the customer and thus at the realization of the two models of utilization control with *DREISAM*. Figure 6.3 shows the time flow of the phases with the parties involved.

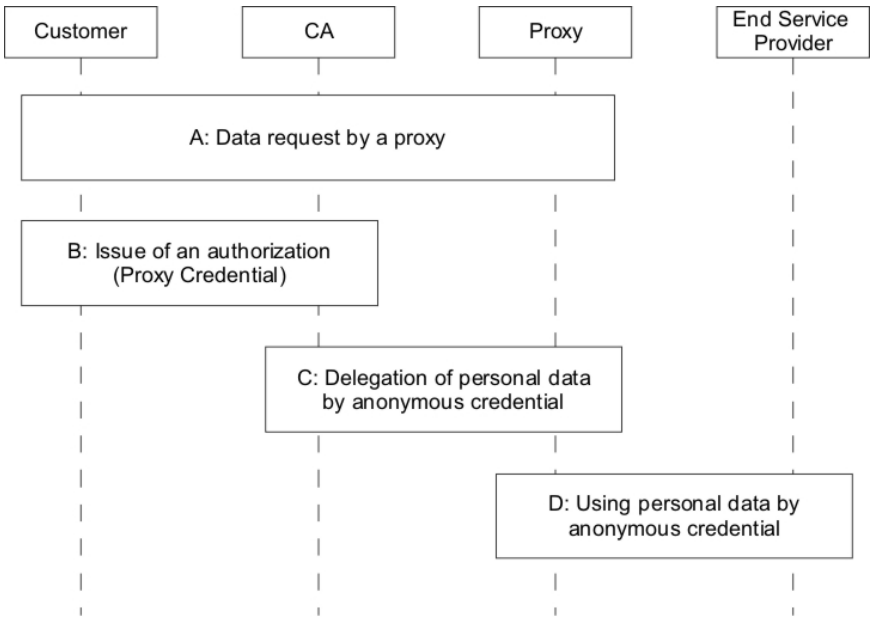

Figure 6.3 The protocol phases of a delegation of an authorisation for the use of personal data or its attributes with *DREISAM*.

6.1.2.3 Revocation Phases of an Authorisation

The aim of a revocation of an authorisation is that the customer data delegated to a proxy cannot be further used. A certification authority should no longer delegate the data concerned to the proxy after a revocation and a service provider should reject an access enquiry of a proxy using this customer data. A revocation therefore applies to the proxy credentials as well as to the anonymous credentials issued for him. The three phases of a revocation are shown in Figure 6.4.

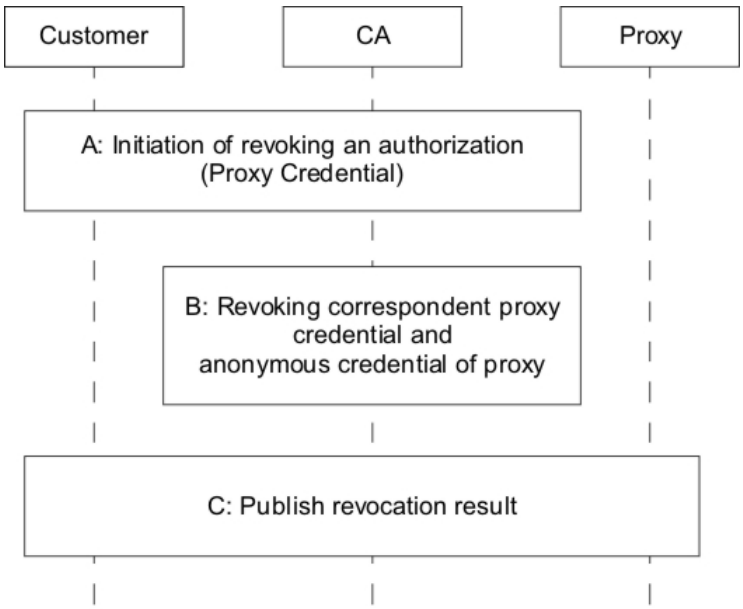

Figure 6.4 The revocation of an authorisation with *DREISAM* in its phases.

The aim of the first phase is the initiation of a revocation with the evidence that applicant is authorised for the revocation. The application is placed at the same certification authority which issued the proxy credential to be revoked. This certification authority subsequently examines whether the applicant is authorised for the revocation. This is the case when he is at the same time the customer upon whose application the authorisation was issued or is the certification authority that accredited the personal data concerned of the customer.

The aim of the second phase is the execution of the revocation of the proxy credential and the pertaining anonymous credentials of the proxy. Current revocation mechanisms for conventional attribute certificates such as revocation lists (Ford and Baum, 1997), are implemented together with the mechanism for anonymous credentials, i.e. the use of a dynamic accumulator according to (Camenisch and Lysyanskaya, 2002).

The aim of the third phase is the publication of the results of a revocation. The revocation of the proxy credential is published as part of the updated CRL. The accumulator is distributed as part of the public key pk_{CA} of the certification authority, via its directory service for example. The prime numbers of the valid anonymous credential is published in the entry E_{add} and those of the revoked anonymous credentials in the entry E_{delete} of the directory service.

6.1.3 Delegation of an Authorisation

The information flow and the interactions between the parties involved in a delegation are described in the following according to the four phases of the protocol.

6.1.3.1 Phase A: Data Request of a Proxy

Phase A is carried out by the protocol steps 1-3, which are shown in Figure 6.5. In the first step, the customer requests a service from a service provider, who is later his proxy. In order to pre-emptively counteract an undesirable linkage of his transactions, he faces his proxy

under a pseudonym. In this case, the pseudonym is pseudonym(U,Proxy). In the second step, the proxy requests certain data of the customer. In the third step, the customer decides about its release. The identity manager of the customer either makes the decision automatically through a predetermined regulation or the customer decides explicitly about the release through an interaction with his identity manager. If the customer decides for the release of the requested data, continuation is made with phase B of the protocol.

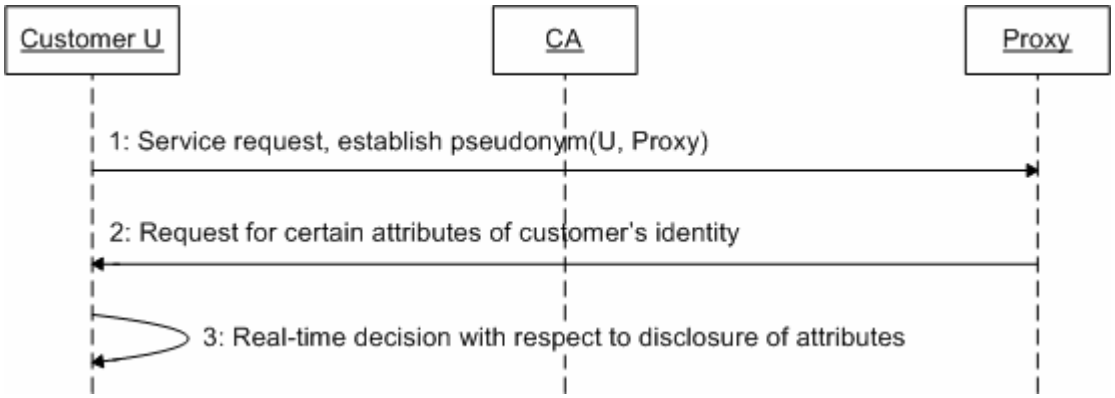

Figure 6.5 Request of a proxy for personal data.

6.1.3.2 Phase B: Issue of an Authorisation

Phase B is carried out by steps 4-14 as shown in Figure 6.6. In the fourth step, the customer requests a proxy credential for his proxy from a certificate authority. With the request, the customer transfers his rules for the delegation and use of the specified data. The rules are specified in his privacy policy for this transaction with the proxy. To protect himself from a linking of profiles over several transactions, the customer faces the certification authority under a pseudonym. This pseudonym is specified in the information flow with pseudonym(U,CA). With regard to the proof of the customer that the data to be delegated belongs to him and takes place in the tenth step and the structure of the evidence protocol from the anonymous credential system (Camenisch and Lysyanskaya, 2001), the pseudonym is generated in the fourth step. This generation is optional and is dispensed with if the customer has already agreed on a pseudonym with the certification authority and wishes to establish a connection with an earlier transaction via the pseudonym. In the fifth step, the certification authority requests the customer for proof of the relationship between this data and himself.

Steps six to nine prepare the evidence in step ten. They deal with the proof that the anonymous credential of the customer for the personal-data concerned has not been revoked. As already described, dynamic accumulators are used for a revocation of anonymous credential. For the proof of a non-revoked credential, these use a witness which is specified in the eighth step as witness w(e(credential(attributes,pseudonym(U,CA))),CA). e(credential(attributes,pseudonym(U,CA),CA)) of the prime number of the anonymous credential thereby corresponds to the personal data attributes of the individuals with the pseudonym pseudonym(U,CA). The witness refers to an accumulator accumulator(v,CA), which is issued and maintained by the certification authority. Whether the witness has to be updated at all, i.e. whether the accumulator has changed, is examined in steps six to eight. In the sixth step, the current accumulator is requested by the issuing certificate authority. To

simplify matters and without loss of generality, it is assumed that it is a question of the same certification authority which was also assigned the delegation. Due to the structure of the anonymous credentials according to (Camenisch and Lysyanskaya, 2001) and assuming that the customer only uses transaction pseudonyms and does not pass on any clear identifying data such as his personal identity number, the certification authority cannot trace back the transactions of the issue of an anonymous credential with the delegation of personal data to the same customer. Since the current accumulator is an integral part of the public key pk_{CA} of the certification authority, in the seventh step, pk_{CA} is sent to the customer. In the eighth step, it is examined whether the witness is up-to-date. This takes place by means of the verification of the accumulator received, which has a serial number for this purpose. If the witness is not in line with the current accumulator, then it is updated in the ninth step. The update (u,e(U,CA)) methods defined are used for this. If the witness is up-to-date, then the ninth step is omitted.

In the tenth step, the customer ultimately proves his relationship with the data to be transmitted by means of an anonymous credential. The ownership of the respective witness and the association of the prime number e(credential(attributes, pseudonym(U,CA),CA),CA) with the current accumulator is proven by a zero knowledge proof procedure. The possibility of the customer sending this prime number to the certification authority for calculating the witness of the presented credential does not apply. Otherwise, the certification authority can trace back the issuance of the anonymous credential with the delegation of the data concerned by way of the prime number to the same customer. In the case where the certification authority does not maintain the accumulator concerned, it must request it from the certification authority CA' responsible in the optional eleventh step.

If the credential is valid, then the certification authority adds an entry into its delegation list in the twelfth step. The list is used as an access control list for the issue of credentials for proxies, i.e. which authenticate themselves with a proxy credential. The access rights correspond to the policy of the customer. The relationship between the entry on the delegation list and the proxy credential is produced by the unique transaction identifier TID. In step 13, the certification authority issues the requested proxy credential for the specified proxy and sends it as confirmation of the procedure to the customer. The proxy credential applies to the public key pk_{Proxy} of the proxy which the customer receives during the authentication of the proxy before the start of the delegation protocol and has transmitted to the certification authority with the application in the fourth step. The customer forwards the proxy credential to his proxy at the end of phase B.

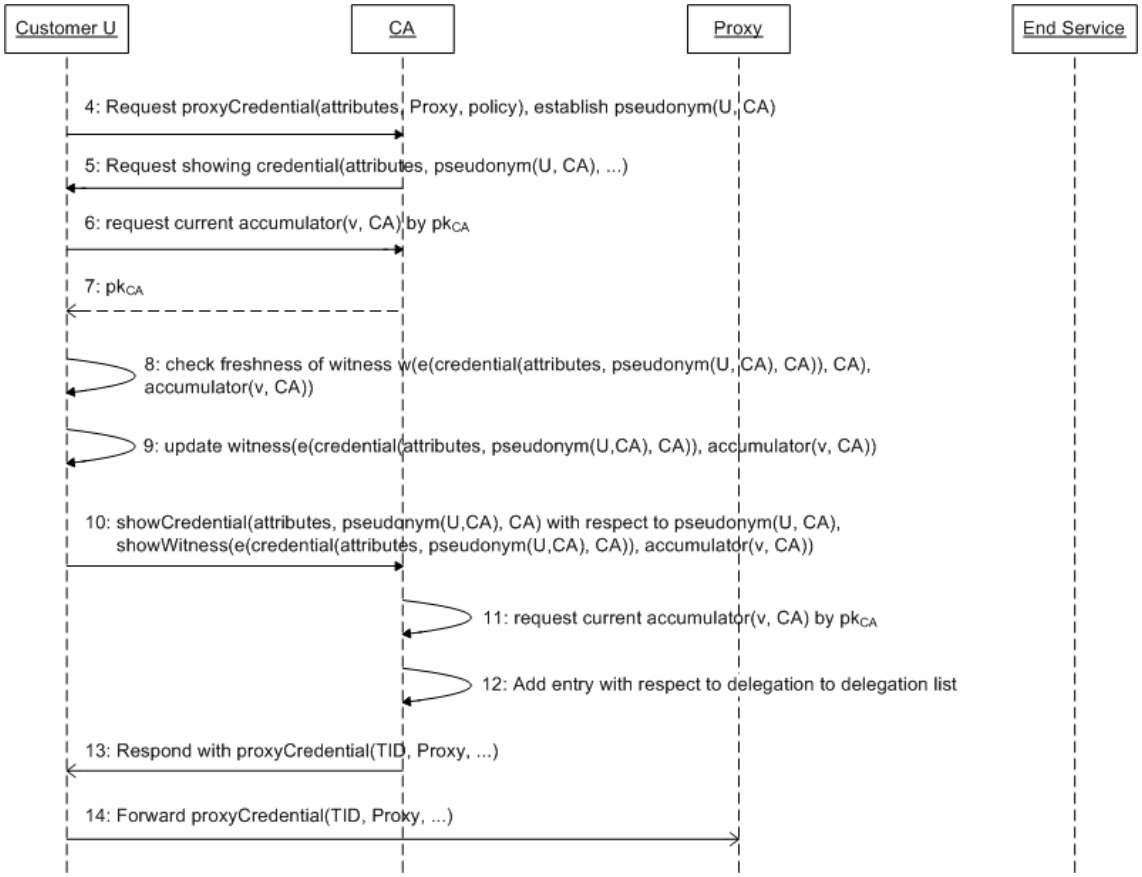

Figure 6.6 Request of the customer for a proxy credential for his proxy.

6.1.3.3 Phase C: Delegation of Personal Data

Phase C is carried out by steps 15-23, whose sequence is shown in Figure 6.7. In step 15, the proxy requests an anonymous credential for the personal data of the customer, to which the proxy credential of the proxy applies. The proxy proves his authorisation to use this data by producing the respective proxy credential. This contains his public key pk_{Proxy}. The proxy proves his relationship with the proxy credential through the digital signature of the application. In addition, he agrees on a pseudonym with the certification authority, to which his anonymous credential is linked. The pseudonym is specified in Figure 6.7 as pseudonym(Proxy,CA). Whether the proxy uses a transaction pseudonym is not taken into further account, as this work concerns the protection of the privacy of a customer. In step 16, the certification authority examines whether the credential of the proxy is valid and whether a release of the data concerned is permitted according to the privacy policy of the customer. This takes place through the comparison of the proxy credential received with the respective entry on the delegation list. The relationship between the proxy credential and the entry is established via the TID. If the credential of the proxy is valid and he is thus authorised for the requested use of the personal data of the customer, then the certification authority creates an anonymous one-show credential with this data, links it to the pseudonym pseudonym(Proxy,CA) of the proxy and sends the anonymous one-show credential to the proxy. The delegation is added to the entry on the delegation list.

Steps 17-22 relate to the issue of the anonymous one-show credential for the proxy. The usage rights for the use of the data are entered in the credential under the *restrictions* field. According to the model of usage control, this can involve both obligations and conditions for the use of this data. A further feature of this credential is the fact that it is a question of an anonymous one-show credential. Multiple use of an anonymous one-show credential is detected by the service where the one-show credential is used for the second time (Camenisch and Lysyanskaya, 2001). The incentive for a proxy to use a one-show credential once at the most lies in the encryption of a secret of the proxy, e.g. his private sk_{Proxy} key, in the credential and its disclosure, conditional on design, in the event of multiple uses. The hidden motive of this measure is to increase the damage of a proxy in a replay attack and thus prevent this type of attack. Further attributes of the credential are the customer data delegates, the pseudonym of the proxy, the name of the certification authority and the period of time in which the credential is valid. The period of time is specified by a commencement and termination date. Step 18 adds the prime number e(Proxy,CA) of the anonymous one-show credential to the accumulator accumulator(v,CA) of the certification authority and step 19 to the directory service entry E_{add}. Step 20 updates pk'_{CA} by the old accumulator being replaced by the new version. Step 21 publishes the updated directory service entry E'_{add} and the new version of pk'_{CA}. The credential produced is sent in step 22 to the proxy together with the new version of the public key pk_{CA}. The key pk_{CA} is sent in the form of a key certificate in order to secure its authenticity. Finally, the proxy produces the witness for this credential. The current accumulator is extracted from pk'_{CA}. Step 23 is optional, but should be executed before the initial use of the credential. It is thereby assumed that the authenticity of the customer data can be shown by the proxy.

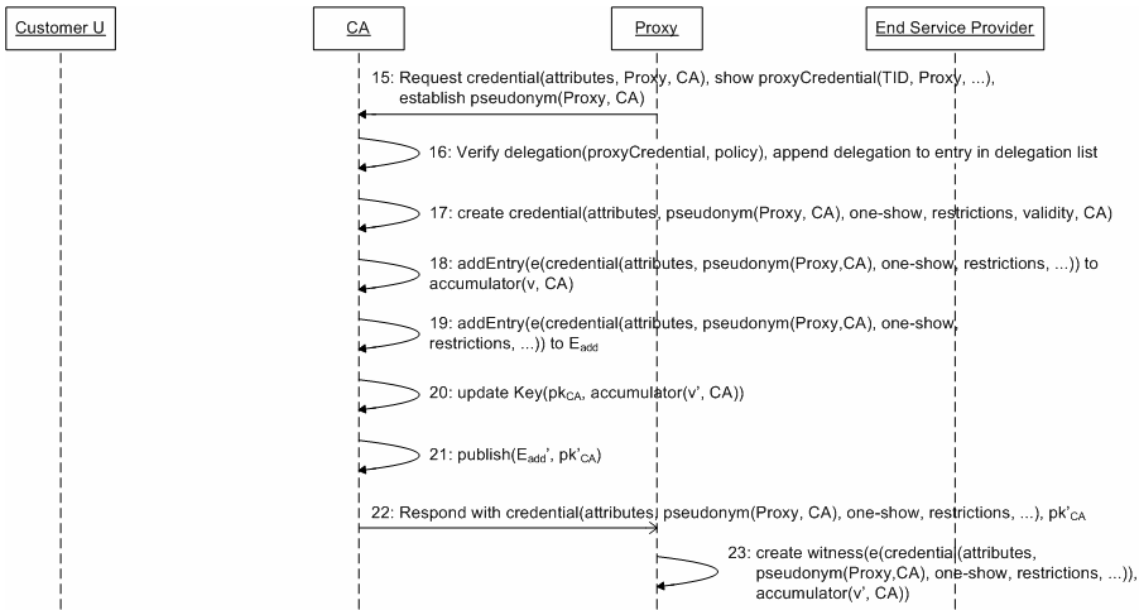

Figure 6.7 Enquiry of a proxy at a certification authority for personal data in the form of an anonymous one-show credential.

6.1.3.4 Phase D: Use of Personal Data

The final **phase D** is carried out by steps 24-33 (cf. Figure 6.8). In step 24, the proxy requests the service of the target service provider and agrees with him upon the pseudonym pseudonym(proxy,end service). The reason for generating this pseudonym corresponds to that of step 16. By means of this pseudonym, the proxy proves to the end service provider in step 32 that the access data, i.e. the customer's data match his identity for this transaction. In step 27, the end service provider requests precisely this evidence. Steps 26 and 27 refer to the examination of whether the proxy's anonymous credential was revoked. This examination takes place in step 32. An accumulator value accumulator'(v,CA) is calculated and compared with the current accumulator value accumulator(v,CA). The target service provider requests the current accumulator value from the certification authority in step 26 and obtains it in step 27. With steps 28 and 29, the proxy obtains the current accumulator value of the certification authority by means of which he examines in step 30 whether the witness value witness w(e(credential(attributes,pseudonym(Proxy,CA),one-show, restrictions,...)),CA) is up-to-date. For this, a witness value witness w' is calculated. The witness value witness w is up-to-date if it is equal to witness w'. In this case, step 31 is omitted. Otherwise the old witness value w is replaced by w'. Step 32 finally conveys the evidence that the access data belongs to the proxy by proving the real-time of the anonymous credentials. On the result of step 32 and the allocation of rights in the end service provider's access control list, in step 33, the proxy is either granted or denied access to the desired service and therewith the function of the service.

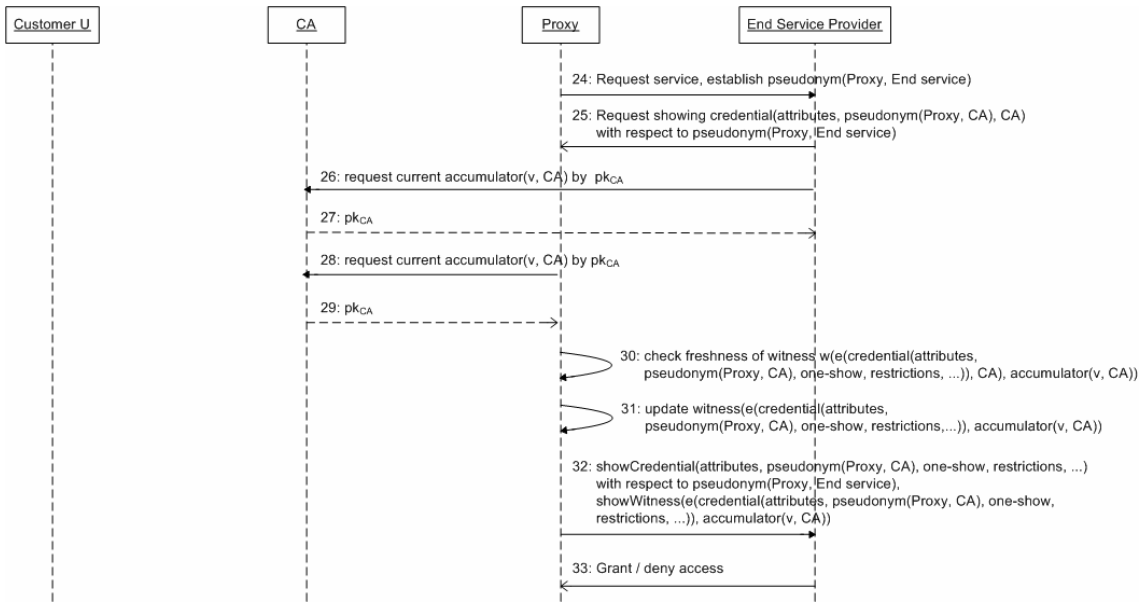

Figure 6.8 Use of the customer's personal data by his proxy for authentication to an end service provider.

6.1.4 Revocation of an Authorisation for Delegated Data

The revocation of an authorisation for the use of the customer's personal data can be the result of various incidents. The revocation initiator varies depending on the event that occurred. A certification authority thus revokes a customer's authorisations and his delegated authorisations if the customer data concerned can no longer be related to him. Examples of

this are the loss of his driving license, a removal and the customer's change of address involved, the change in family status and the membership of a health insurance fund. In this case, the data transmitted is no longer up-to-date and therefore no longer corresponds to the customer's physical identity. Depending on the relation of the application, the customer's access rights to services and with them those of his proxy can change. Furthermore, the authorisations are revoked if the customer proves to be a fraud. The case where a customer revokes delegated authorisations arises when the purpose of the delegation has been fulfilled before the planned termination or his proxy abuses the delegated data. It is assumed in the following that a customer revokes a delegated authorisation. In the other event, the customer is replaced in the protocol sequence by the revoking certification authority or the protocol begins with phase B when it is a question of the same certification authority.

In general, a revocation of an authorisation applies to the pertinent proxy credential and all the anonymous credentials that have been issued on the basis of this proxy credential. It is furthermore the aim that no identifying data on the customer accumulates by means of which his transactions and thereby his profiles can be linked without his agreement. This goal is only pursued, however, when the customer is honest.

6.1.4.1 Phase A: Initiation of a Revocation

Protocol steps one to eight form the initial revocation phase of an authorisation. Figure 6.9 presents their sequence. In the first step, the respective proxy credential is transmitted with the revocation request to the certification authority. With the proxy credential specification the certification authority is able to identify the delegation concerned and the pertaining anonymous one-show credentials. The clear identification of the entry on the delegation list takes place via the TID. In addition, the customer specifies with the application the desired point in time (revocationTime) at which the authorisation and the anonymous credentials connected should be revoked. The customer faces the certification authority under the pseudonym pseudonym(U,CA). The pseudonym is identical to the pseudonym that the customer has used for the request for an authorisation. This does not affect the customer's privacy since the transaction for a revocation must be linked with the request transaction for an authorisation in order to be able to identify the anonymous credentials of the delegation.

In the second step, the certification authority selects the anonymous one-show credentials and the proxy from the delegation list. For this, the TID is used which, at the same time, is the unique identifier of an entry in the delegation list. However, before a revocation is made, the certification authority makes sure that the customer with the pseudonym pseudonym(U,CA) is authorised for this revocation. The customer is therefore requested in the third step to prove the relationship between himself and his personal data, to which the revoking authorisation refers. Analogous to phase B of the *DREISAM* delegation protocol, the following steps apply to the examination and, if necessary, updating of the witness value w(e(credential(attributes ,pseudonym(U, CA),CA)),CA) and the proof of the anonymous credentials credential(attributes, pseudonym(U,CA),CA) for the pseudonym pseudonym(U, CA).

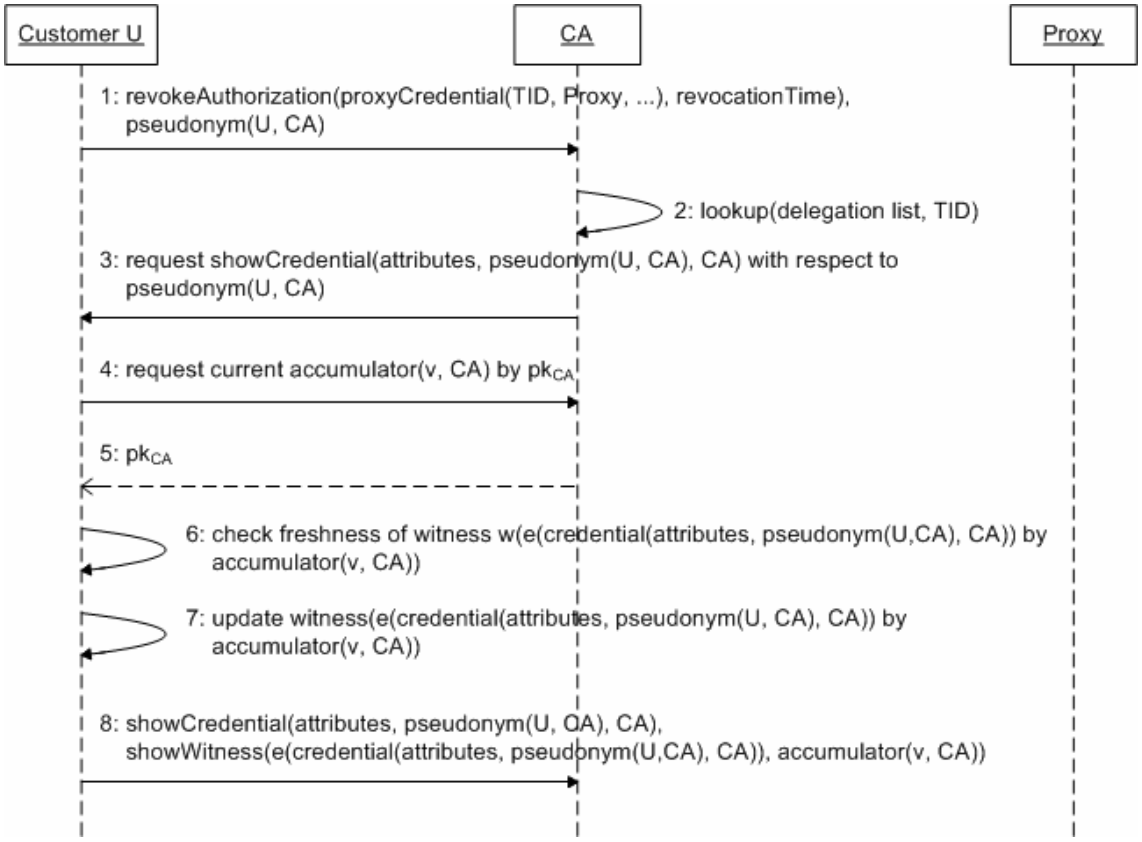

Figure 6.9 The customer initiates the revocation of an authorisation for the use of delegated personal data.

6.1.4.2 Phase B: Revocation of Credentials

The result of steps nine to twelve is the revocation of the credentials for delegated authorisation, i.e. the credential of the proxy, and for the data delegated to the proxy, i.e. his anonymous one-show credentials. All steps are carried out by the certification authority (see Figure 6.10). Since a proxy credential is produced in the form of an attribute certificate according to (Farrell and Housley, 2002), the revocation mechanism of a PKI can be used (Ford and Baum, 1997). Since the development of revocation mechanisms is not the central focus of this work, a Certificate Revocation List (CRL) is used. This revocation mechanism is not necessary for the basic functionality of the protocol and can be replaced by alternative mechanisms. In the ninth step, the certification authority adds the respective proxy credential to the revocation list. In the tenth step, all anonymous one-show credentials of a proxy that were issued on the strength of the revoked proxy credential in the ninth step are revoked. The following steps are executed for each of these anonymous proxy credentials:

- **Step 10.1:** The prime number e of the anonymous one-show credential credential(attributes,pseudonym(proxy,CA),one-show,..., CA) is removed from the current accumulator accumulator(v',CA) of the certification authority.
- **Step 10.2:** The prime number *e* is removed from the directory service entry E_{add} of the prime numbers of valid anonymous credentials and

- **Step 10.3:** added into the directory service entry E_{delete} of the revoked anonymous credentials.

In the eleventh step, the certification authority updates its accumulator and subsequently adds it to his public key pk_{CA}. If all the protocol steps of phase B have been correctly executed, then the delegation entry on the delegation list is marked as revoked with the point in time of the revocation (revocationTime). Later requests of a service for personal data for which the revoked proxy credential is used are seen as invalid.

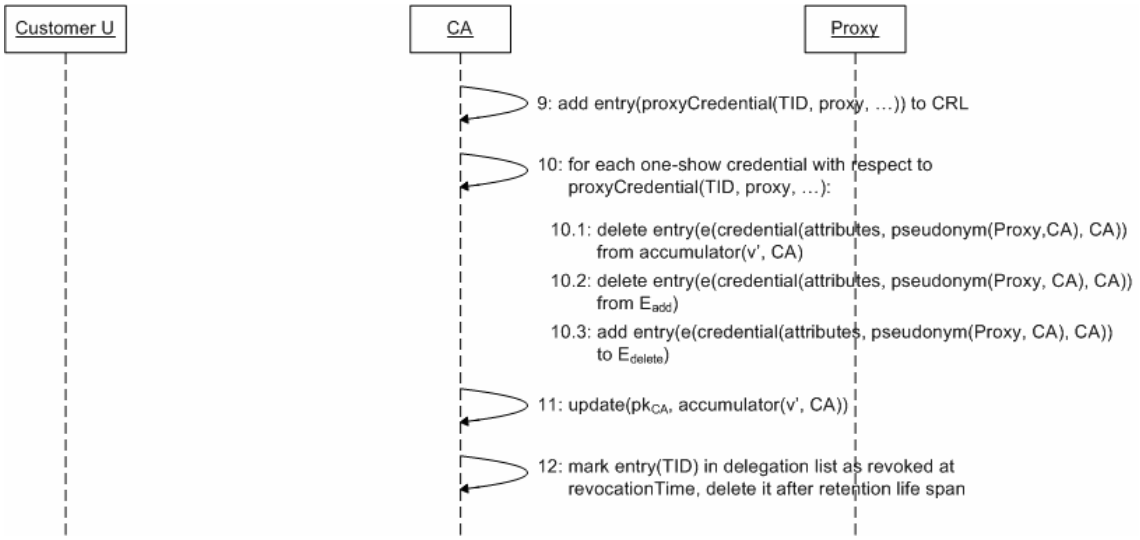

Figure 6.10 The certification authority performs the revocation of the proxy credential and the pertaining anonymous credential.

6.1.4.3 Publication of the Revocation Results

The last phase publishes the revocation in steps 13-17 (see Figure 6.11). Step 13 releases the updated directory service entries for publication. A consistent database of the public directory service is ensured through the simultaneous publication of these values. In response to the initiator of the revocation, the certification authority returns the result of the revocation together with the up-to-date accumulator as part of pk_{CA}. The result of the revocation is revoked in the event of success and otherwise denied. Step 15 is then carried out if the anonymous credential for the customer's data has been revoked. In this case, the customer updates the witness value for this credential depending on the accumulator received from step 14. Step 16 sends the result of the revocation to the proxy so that he can update his witness values for the relevant anonymous credentials in step 17.

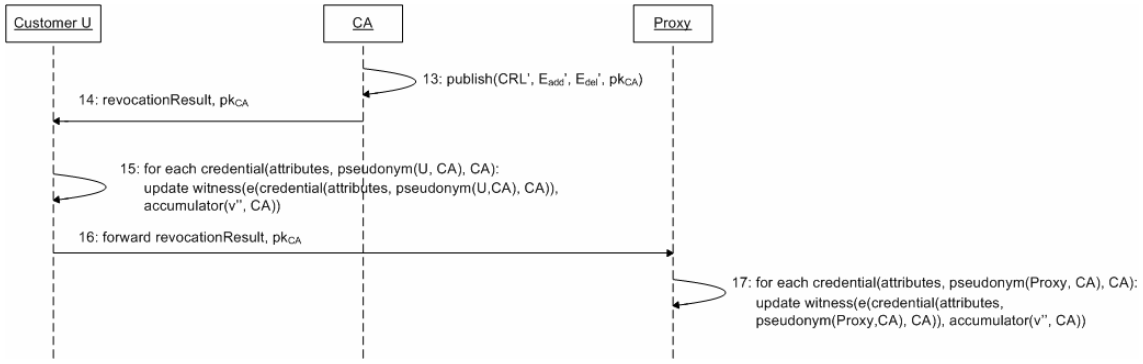

Figure 6.11 Publication of the revocation results.

6.1.5 Security Properties of *DREISAM*

The assumption which has to been proven is that *DREISAM* (a) does not disclose any personal data of the customer, (b) the transactions of a customer cannot be linked, and (c) a proxy is only able to use customer's personal data according to the purpose of the corresponding business process. Cases (a) and (b) refer to a controlled disclosure of personal data; case (c) refers to a prevention of abuse. Additionally, disputes must be resolvable to clarify liability.

6.1.5.1 Controlling Disclosure of Personal Data

Since *DREISAM* makes use of the identity manager *iManager*, a user is able to disclose his personal data as partial identities relating to the service provider and the service as well as stored personal data is the protected store of the *iManager*. Non-linkability of transactions is achieved by using a pseudonym only for one transaction and by using anonymous credentials. Non-repudiation of a delegation is achieved by the log in the delegation list of the corresponding CA. Non-repudiation of a service use is achieved by showing a credential and by the access log of the corresponding service provider. As the investigation on identity management systems, especially of *IBM idemix*, shows, a delegation of anonymous credentials implies that a customer lose control about his identity, *DREISAM* enables a customer to delegate specific personal data to a proxy by using proxy credentials. This empowers a customer to delegate least attributes necessary for the purpose of a proxy. The de-anonymisation mechanism of *IBM idemix* is used for revealing the identity of a customer or his proxy in case of fraud.

6.1.5.2 Preventing Abuse of Disclosed Personal Data

If a service provider grants access to his service to a proxy whose credential is not specified for this service, the service provider would grant access to an unauthorised party. This contradicts with the security interests of end service providers and his motivation to use an access control. From this contradiction it follows that end service providers will follow the restrictions of an anonymous one-show credential. Double-spending of a one-show credential is detected, if the end service provider checks on-line with a certification authority whether the shown credential has already been used. In the off-line case, such a double-spending cannot be prevented but it can be detected afterwards by the same way as in the on-line case. With respect to undesired re-delegation of a proxy credential, the certification authority would issue an anonymous credential for another party which is not mentioned in customer's policy.

It follows that this certification authority does not follow the certification policy and is not trustworthy. This contradicts the assumption of a trustworthy certification authority.

6.1.5.3 Solving Disputes

Disputes between a customer and a proxy relating to the use of personal data may occur in two cases. A proxy uses a delegated credential of the customer and denies its use or a criminal customer uses a credential in the name of a proxy and denies its use. A dispute is solved by a certification authority based on the transcript of a delegation transaction and the log of the corresponding end service provider with respect to the access queries. The certification authority compares the transcript of the credential use with the transcript of issued credentials to identify the identity of the cheater.

6.1.6 Applying *DREISAM* on Loyalty Program with Delegation of Rights on Customer's Data

The application of *DREISAM* in order to prevent linkability of customers' profiles by merchants in this case study has two stages:

1. **Premise:** To prevent linkability when showing a loyalty card, anonymous credentials are used for realizing a loyalty card.
2. **Unlinkable Delegation:** *DREISAM* delegation protocol is used for delegating an access right in order to read a specific entry of customer's profile at the loyalty program provider.

The application of the first stage is shown in Figure 6.12. In this case study, a customer has solely one loyalty card of one loyalty program. By using anonymous credentials, a customer is able to use his loyalty card with different pseudonyms and to hide identifying data, e.g. his card number, if it is not necessary for the service. If the card number is needed, e.g. to deposit premium points on customer's profile, the card number is hidden in the showing protocol and it is sent to the loyalty partner provider via the merchants by means of an encrypted card number: $enc(pk_{\text{Loyalty program provider}}, \textit{Card ID} \parallel pseudonym_{\text{Supermarket}})$. If the encrypted card number, the cipher text, is in every transaction the same, merchants and the CA are able to trace this customer by this cipher text. To avoid linkability by the encrypted *Card ID*, the cipher text has to be randomised each time the loyalty card is going to be delegated. This can be achieved by using the encryption scheme of the payment protocol family *i*KP (Bellare, Gray, Hauser, Herzberg, Krawczyk, Steiner, Tudsik and Waidner, 1995). The plain text, *Card ID* and the associated pseudonym which the customer has used at the supermarket, is encrypted with a one-show random number (SALT) by an XOR-operation and finally asymmetrically encrypted with $pk_{\text{Loyalty program provider}}$. The loyalty program provider does not need to know SALT in advance, since he is able to reconstruct it after he has decrypted $enc(pk_{\text{Loyalty program provider}}, \textit{Card ID} \parallel pseudonym_{\text{Supermarket}})$. So, only the loyalty program provider is able to encrypt the card number by his private key $sk_{\text{Loyalty program provider}}$ and to know the relationship between pseudonyms of a customer and his unique card number which is used to identify the customer and the data base record of his profile.

The transactions in Figure 6.12 cannot be traced back to the customer by the merchants, if there is no intersection in the disclosed data. The customer uses different pseudonyms *4711'0815*, *1024*, and *Abcd'23* in combination with his loyalty card as an anonymous

credential. Since an anonymous credential hides its data, it is shown in Figure 6.12 in brackets.

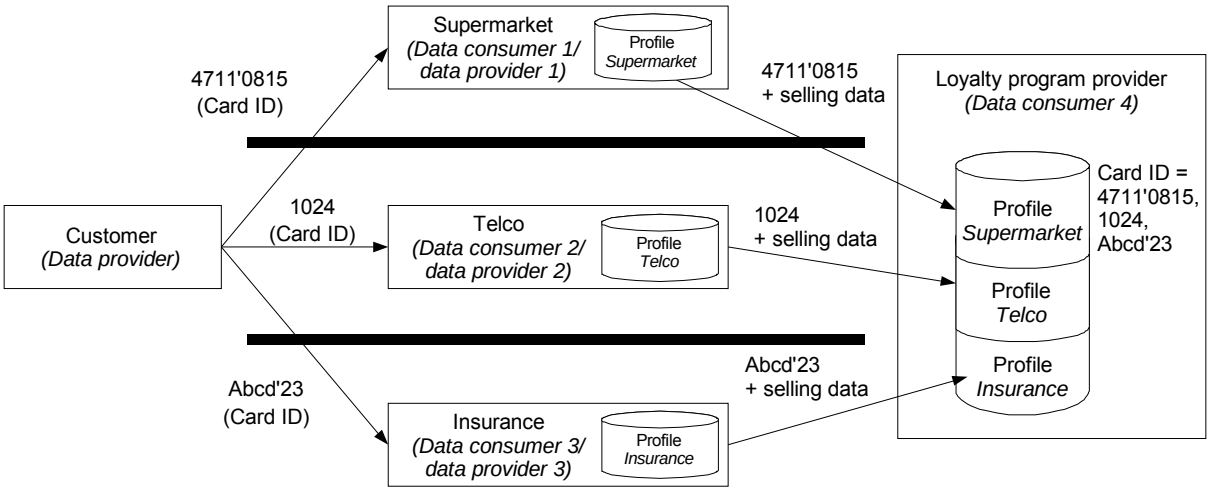

Figure 6.12 Applying anonymous credentials for a loyalty card to prevent linkability if showing a loyalty card.

The principle of an unlinkable delegation of rights by using *DREISAM* is shown in Figure 6.13. A certification authority extends the model with regard to the *DREISAM* model. The role of a certification authority is taken by a new organization according to the model, even thought the loyalty program provider could also be in the role of the CA. The suggestion is to divide the loyalty program provider and the CA in two organizations. Firstly, the role of a CA is not the core competence of a loyalty program provider. Secondly, other loyalty program providers would probably not accept a CA who belongs to a competitor.

The trust relationships between the participants are as follows:

- The loyalty program provider trusts the CA that the CA certifies the relationships between customers and loyalty card as well as between merchants and proxy credentials according to her certification policy.
- Merchants trust the loyalty program provider that he issues valid loyalty cards.
- Customers trust the loyalty program provider that he manages customers' profiles confidentially and discloses them solely if the corresponding customer has given his authorisation and if this authorisation is valid. Furthermore, customers trusts the CA that she issues proxy credentials according to her certification policy.

The customer uses the pseudonym *klf2007* in order to remain unlinkable between the transaction with the insurance company and those with the pharmacy in the past. After the request of a merchant (insurance company) for accessing the profile pharmacy of the customer (phase A of *DREISAM*), the customer requests the corresponding authorisation for the insurance company at a certification authority. The result of step two, which is phase B of *DREISAM*, is the authorisation for the insurance company realised by a proxy credential. A customer has to show that his pseudonym *klf2007* belongs to the pseudonym used at the supermarket (*4711'0815*). Showing this relationship may not lead to disclose the customer's

pseudonym with regard to the supermarket to the CA. Otherwise the CA is able to identify customer's profile at the supermarket. Latter can be achieved by using a key-oblivious verifiable encryption scheme similar to (Camenisch and Lysyanskaya, 2001). Showing the relationship between two pseudonyms in a PKI with anonymous credentials means to show that they are both based on the same secret key $k_{Customer}$. This authorisation is forwarded in step three. Step four represents phase C of *DREISAM*: the insurance company, a proxy of the customer concerning the access on customer's profile at the loyalty program provider, requests the copy of customer's loyalty card by showing his corresponding proxy credential as the authorisation for this copy. By getting the copy of customer's loyalty card, the insurance company is allowed to access customer's supermarket profile in step five. Step five represents phase D of *DREISAM*. The relationship between the pseudonym *klf2007* and the *Card ID* is again introduced to the loyalty program provider by the encrypted *Card ID* together with a random number nonce: $enc(pk_{Loyalty\ program\ provider}, Card\ ID \parallel pseudonym_{Supermarket})$

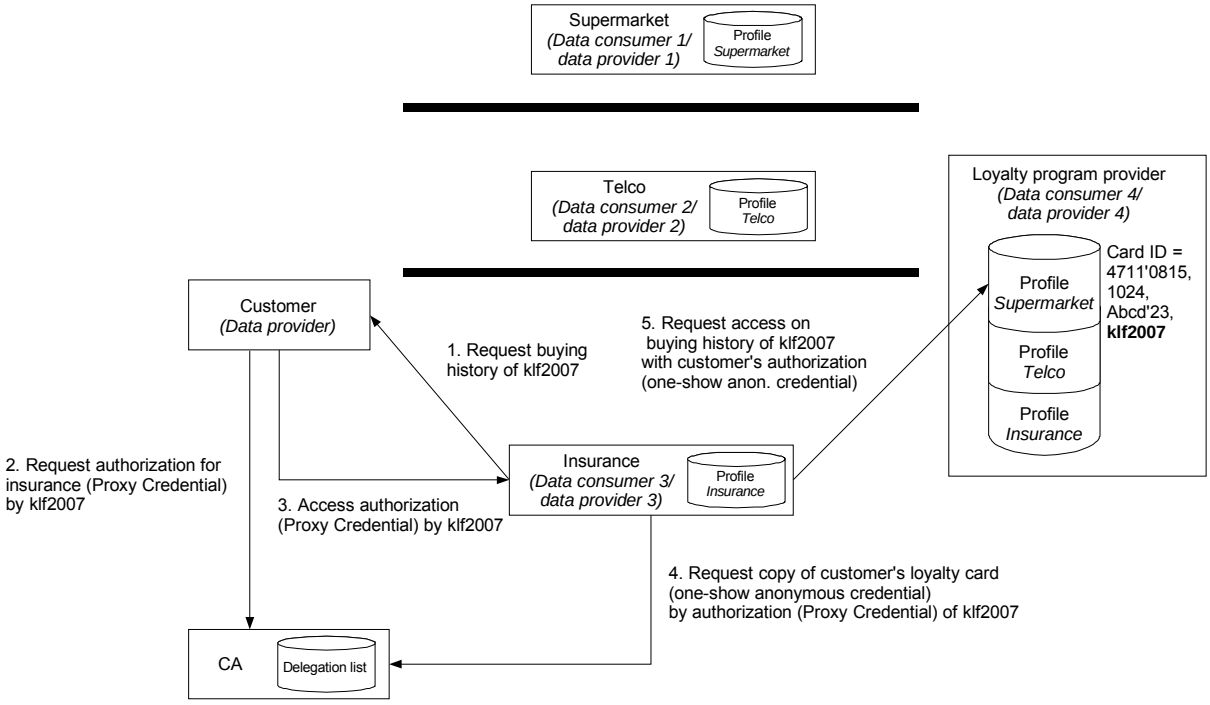

Figure 6.13 Applying *DREISAM* for an unlinkable delegation of access right in principle.

6.1.7 Conclusion

DREISAM extends identity management by a usage control mechanism. It is now possible to specify a desired use of delegated personal data according to the privacy interests of customers. A customer remains thereby unlinkable so that he is further on able to decide on the access on his personal data. *DREISAM* makes thereby use of the identity manager *iManager* in combination with the anonymous credential system *IBM idemix*. However, a customer is able to specify the desired use of his data by an authorisation; he cannot control the enforcement of this authorisation, since he has no access on the information system of participating certification authority and service providers.

As shown in the case study *Loyalty Program*, DREISAM prevents profiling if a customer delegates access rights on his profiles, which are externally stored, to service providers. A loyalty program provider benefits from preventing undesired profiling of customers' by using *DREISAM* in combination with identity management, since the loyalty program provider is the only provider who knows all profiles of each customer in a loyalty program, even if customers' delegate access rights to loyalty program partners for personalised services.

6.2 'Data Track' for Increasing Transparency for End Users

Being able to track what data were disclosed, when, to whom, and how the data are further processed, is an important feature to provide transparency of personal data processing.

Within the EU FP6 Project PRIME, which develops a working prototype of a privacy-enhancing and user-controlled Identity Management System, this data logging and tracking function is implemented in the so-called "Data Track". The Data Track is currently extended to also advise users about their rights and enable them to exercise their basic rights to access data, or to rectify and request their deletion online, and help them to check on agreed obligations or to set obligations.

The privacy principle of transparency is an important prerequisite for users for having control over their personal spheres. Furthermore, also for enhancing trust in privacy-enhancing technologies, the users should feel in control of the technologies concerning them, which could for instance be achieved if procedures are transparent and reversible (see (Andersson, Camenisch, Crane, Fischer-Hübner, Leenes, Pearsson, Petterson and Sommer, 2005).

In this section, we will discuss the legal foundations of the Data Track function, present its logging and search functionality and its online help functions which enable users to exercise their rights and to keep control over personal data which they have released.

6.2.1 Legal Background

A society, in which citizens could not know any longer who when and in which situations knows what about them, would be contradictory to the right of informational self-determination and thereby informational privacy. Hence, the privacy principle of transparency of personal data processing is a key to informational self-determination. For this reason, the EU Data Protection Directive 95/46/EC guarantees data subjects extensive information and access rights:

According to Art. 10 of the Directive, individuals from whom personal data will be collected have to be informed about the identity of the controller, the purposes of the data processing, and about further information in so far, as such further information is necessary to guarantee fair data processing, including the existence of the right of access to and the right to rectify personal data.

Pursuant to Art.12 of Directive 95/46/EC, an individual has the right to access, i.e. the right to obtain from the data processor:

- a confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; and

- communications to him in an intelligible form of the data undergoing processing and of any available information as to their source.

In addition, Art. 12 grants individuals the right to obtain from the controller the rectification, erasure, or blocking of data concerning them each time the processing does not comply with the requirements of the Directive, in particular when the data at issue are incomplete or inaccurate.

Art. 14 ensures that data subjects are aware of the existence of the right to object e.g. to data processing for direct marketing.

6.2.2 Logging Functionality

The Data Track allows users to "track" their personal data that they have released to other sites via data records kept at the end user's side and via compiling requests for information on recording done at the services site.

It stores transaction records comprising personal data sent, date of transmission, purpose of data collection, recipient, and all further details of the privacy policy that the user and the recipient have agreed upon (see also (Pettersson, Fischer-Hübner and Bergmann, 2006)).

A legal requirement for requesting data from a data subject is, as noted above, that information about the request (at least the identity of the so-called controller and data processing purposes) is available to the data subject before data disclosure. With PRIME enabled systems on the end user's side, no data should be released if such information cannot be obtained from the services site. This makes it also possible to record this information at the user's side in form of a so-called privacy policy under which the data were released. We want to stress the importance of recording this privacy policy which should contain the premises for how the collected data are used and stored: it would constitute a valuable document in case a user feels that something is wrong with how his data have been used. Presently, users may inspect privacy policies published on web sites but if they later on come back to these web pages, they cannot be sure that the same version is still available. This severely restricts transparency. Also negotiated obligations, such as "delete my address after six months" or "notify me whenever my address is sold to another organisation" and "let any third party organisation use my address only once", should be added to the stored privacy policy.

In order to make the log files useful for the user, some other information has to be added, such as the pseudonyms used for transactions. By authenticating via a pseudonym a user can in principle identify himself as a previous contact but still be pseudonymous, or if he is not pseudonymous at the current contact, he can at least use the pseudonym employed at that time to demonstrate that it was him who previously released personal information. Also the credentials disclosed or received are as important to store in the transaction record as other types of personal information. They will, at a later time, facilitate the re-identification of the user, and as such belongs to a well-functioning identity management system even without a history function such as the Data Track. For exercising legal rights using the Data Track (see below), users need to have records where individual data items are stored in relation to the conditions of each transaction. There should also be a possibility for users to label transmission records in order to group them in a meaningful way ("Holiday 2006" includes both travel and hotel bookings) and add comments ("I phoned them to make clear that all our children are under 12"). This is not necessarily performed at transaction time, and thereby not

purely a logging function, but from the user's perspective it makes sense to see this information as part of the transaction records.

6.2.3 Search Functionality

As people engage in many transactions, which may involve multiple providers simultaneously, the implementation of a usable Data Track is difficult from an HCI perspective. Providing users with easy tools to finding relevant data disclosure records is one example. In PRIME several ways are considered as it will be discussed in this subsection.

Two search methods are quite straightforward and might appear as the obvious choices: (1) Sorting step-wise by categories, such as 'Personal data' and 'Receivers'; and (2) Simple search box. However, these two approaches seem unsatisfactory because users are unaware of what the system does as revealed in user tests performed by the PRIME group. More suitable methods that are currently pilot-tested include: (3) Template sentences which put search boxes within meaningful frames: "Who has received my [drop-down list with data]?" (4) A scrollable transaction track that shows all the records at once. The records are shown in abbreviated form as small pages stacked along a timeline (see Figure 6.14). A slider provides the possibility to highlight an individual page in the stack. In this way, users could browse through the records without having to understand sorting or to articulate refined search requests.

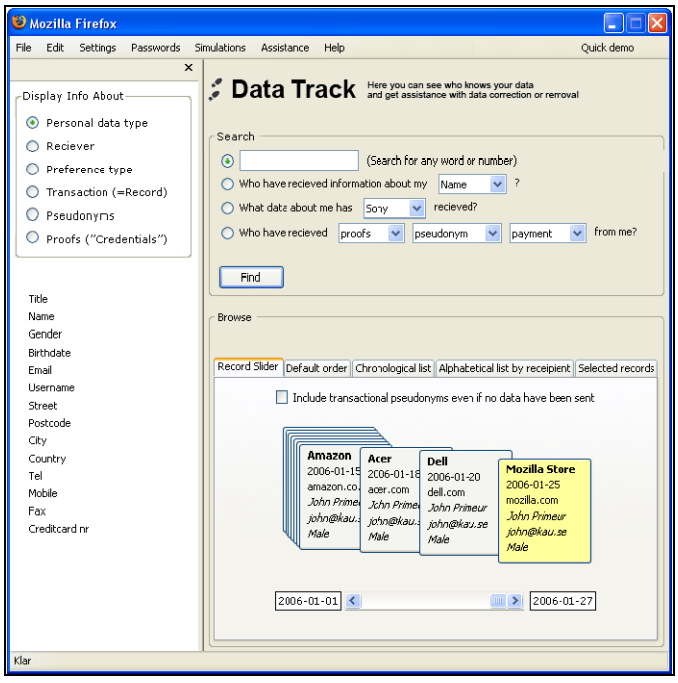

Figure 6.14 Data Track window including template sentences and scrollable tracks.

Obviously, this method seems more appropriate for the beginner whose amount of transaction records will be limited. For the more advanced user combinations of methods have to be explored and developed (see also (Pettersson and Fischer-Hübner, 2006a; Pettersson and Fischer-Hübner, 2006b).

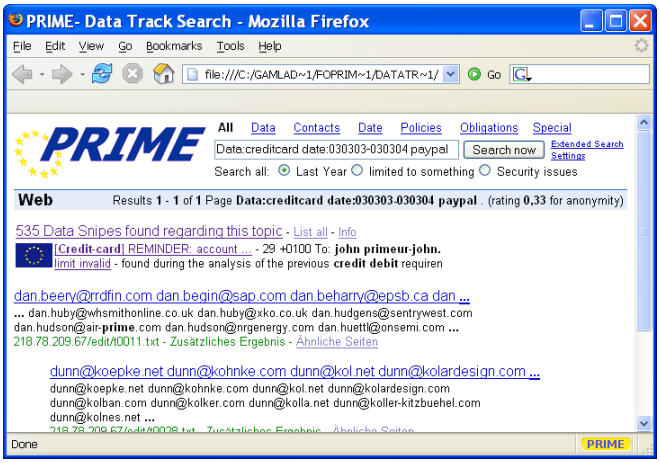

Figure 6.15 Tentative Data Track window in web search engine style.

As far as more experienced users may be familiar with an approach similar to a web search engine (see Figure 6.15) we propose such an additional “advanced search” option. The filtering options might be a difficult for lay users to understand. Possibly, specific privacy-related key words (such as ‘date’, ‘order’, ‘buy’, ‘contact’, ‘payment’/’cost’) can be used for filtering or grouping search results. Experiments should evaluate the usefulness of this approach. Due to the lack of availability of a real and huge data pool, we have to postpone this task into a later stage of the PRIME project.

6.2.4 Support for “Worried Users”

Sociological research on trust has shown that trust in a service provider can be increased if procedures are transparent, reversible, and in case of breaches of trust there are means of redress (see also (Andersson, Camenisch, Crane, Fischer-Hübner, Leenes, Pearsson, Petterson and Sommer, 2005)). This can be provided by the Data Track. However, users might not necessarily believe that the Data Track can offer sufficient help. For instance, a test subject of usability tests performed at Karlstad University said about the Data Track function of the tested UI mockups “Even if it is good to see what information has been sent, it is too late anyway because you cannot undo it.” This is however not really true, because users in Europe still have basic legal rights according to EU Directive 95/46/EC to access, block, rectify or delete data under certain circumstances (see above). Here we have a case where the user interface really can reinforce trust. Our user tests have shown that many people seem to be unaware of these rights. Hence, it is important that the Data Track function also informs users about those rights, and should contain online functions for exercising these rights. It should be also possible to track the fulfilment of agreed obligations via the Data Track interface. Help functions could also inform about available external help, as users may doubt that the system per se can help them all the way through all conceivable situations. One could compare wishes surfacing in user studies that e-commerce companies should provide “Access to helpful people” (Nielsen, Molich, Snyder and Farrell, 2000). The Data Track UI should therefore also provide access to up-dated information on consumer organisations and/or data protection authorities that can help with legal issues.

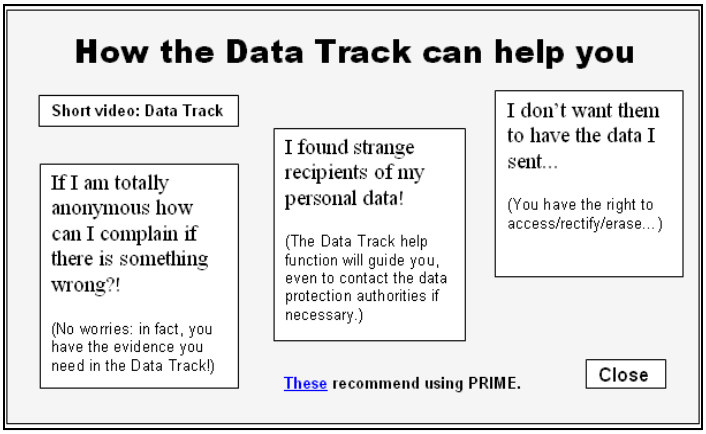

Figure 6.16: "Quick demo" window

Figure 6.16 sketches a "Quick demo" window accessible via the "Quick demo" menu of the Data Track UI (see Figure 6.14), which provides help for "worried users" by informing them about their rights, how to exercise their rights offline or online via the Data Track (see below) and contact addresses for help. The text boxes in the "Quick demo" window are clickable buttons leading to the assistance functions.

6.2.5 Online Functions for Exercising Rights

The Data Track allows users to easily track what personal data items have been released to whom under which conditions. For released data items, it also provides online functions for users to allow them to easily exercise their rights to obtain from the services site the correction and/or erasure/blocking of data concerning them. Once that a user has "tracked" a specific data record, the Data Track user interface provides buttons that the user can click for activating such online functions (see Figure 6.17).

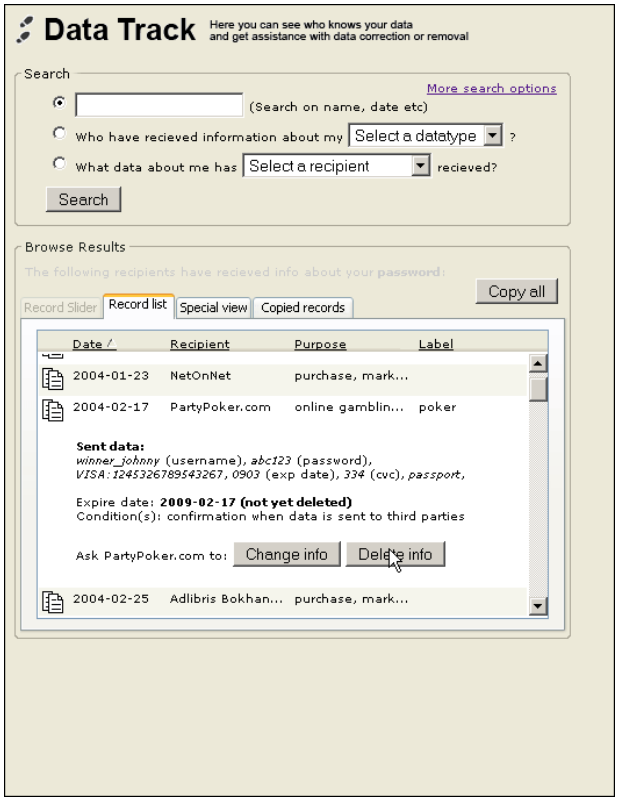

Figure 6.17: Buttons for requesting correction or deletion of personal data records.

Online functions for accessing personal data at the services sides are also provided via the "Assistance" menu (see menu bar in Figure 6.17). The user's right to access data allows the user to get also an overview of data that a service provider has compiled out of released data items, such as for instance profiling or scoring information. Besides it allows users to check whether data release policies and obligations are followed by the services sides as agreed upon at the time of data release.

The Independent Centre for Privacy Protection (ICPP) is currently specifying requirements for a "Request PII-related information" online function. Such an online function should assist the user to specify all information needed for a data access request, which comprises:

- The contact address of the recipient.
- The personal data requested: Even though the user has the right to request access to all information that can be linked to him, the user might often only be interest in data that he released or that were collected about him in a specific context. Hence, the online function should also help the user to specify this context, which might also make it easier for the services side to retrieve the data in its databases. If a user has released data under a certain pseudonym, a proof has to be given that the requesting user is actually the holder of this pseudonym.

If the user requests access to data that were obtained directly from him, all this information can be compiled from his Data Track's transaction records. With the help of this information, the "Request PII-related information" online function should compile an access request, e.g.

via email, and send it to the respective recipient. Additional information revealed by the request should be minimised; e.g. if the user's email address has not been released yet, the user may choose another channel instead of email communication or make use of one-show email addresses or other anonymising services.

If no or only an incomplete answer is received from the services side, the Data Track should provide the option to compile a complaint mail to be sent to the supervisory authority in charge.

6.3 Conclusion

Privacy could only be preserved in single-stage business processes and if personal data is explicitly requested by service providers. But in business processes with delegation of rights and in environments in which personal data is collected without asking for customers' consent, customers' has no control on the disclosure of their personal data. The two security mechanisms *DREISAM* and *Data Track* are approaches to give customers' their control back. *DREISAM* prevents profiling with delegation of rights by realising a usage control based on credentials. Concerning unlinkability, customers only have to trust the service provider who manages their profiles. *Data Track* is a history mechanism to retrace the disclosure of personal data for its user. Thereby, *Data Track* supports the privacy principle of transparency of personal data processing.

Privacy is further on based on trusting the service provider who has got identifying data of their customers. To support the growing of trust relationships between customers and service providers, the processing of disclosed personal data should be verifiable for the corresponding customers. The following chapter introduces further work on security mechanisms to enable such verification.

7 Conclusion and Outlook

The mandatory presumption for privacy in business processes with personalised services was up to now customers' trust in the participating service providers. The process models, which are considered in this study, for privacy-aware business processes, suggests an internal access control on customers' data and the application of information security management process models for data protection. Concerning undesired profiling, both approaches require also that customers trust their service providers with respect to the processing of customers' data.

As far as personalised services are realised by single-stage business processes and do not require identifying data of their customers, profiling can be prevented by disclosing different partial identities in combination with different pseudonyms. This is technically supported by current user-centric identity management systems.

By the change of personalised services towards an unconscious collection of customers' data, e.g. in sensor networks, and multi-stage business processes where profiles are externally managed and have to be delegated to service providers, privacy cannot furthermore be preserved by current identity management systems. Concerning re-tracing an unconscious collection of customers' data, the technical integration of data protection legislation in devices is proposed by the term 'Ambient Law'. An approach for a re-tracing mechanism is shown by the 'Data Track' mechanism. Concerning an undesired profiling in multi-stage business processes protocols for an unlinkable delegation and revocation of access rights on customers' profiles are proposed by *DREISAM*. Regarding profiling, the added value is that customers only have to trust the service providers which manage their profiles. Since *DREISAM* does not preserve privacy if the requested data unambiguously identify the customer, this customer has to trust this service provider further on.

Further work investigates on the verification of service providers whether they have processed customers' data according to the negotiated arrangement between service provider and customer as well as according to the given data protection legislation. The aim is to get evidences concerning the use of customers' profiles. In order to technically re-trace the information flow of services, the study D14.3 "Study on the suitability of trusted computing to support privacy in business processes" of the FIDIS work package 14 "Privacy in Business Processes" investigates on trusted computing as a platform to support the enforcement of privacy policies by service providers. By providing mechanisms for user-controlled access control and audit of private data, users are enabled to decide on the disclosure and use of personal data in business processes with proxies. In Information Filtering scenarios occurring e.g. in Recommender Systems, however, private data has to be collected and processed in order to provide the desired results, such as individualised content. In this case, the mechanisms described in this study may be used to prevent entities other than the actual service provider from acquiring private data, but they cannot be used to prevent the service provider itself from using the acquired data in a privacy-invasive manner.

Feasible solutions for privacy-preserving Information Filtering are either based on additional trusted parties or on trusted computing. In the latter case, the parts of an application that are actually used for processing private data have to be realised as trusted software, i.e. they have to be based on a trusted computing platform. Thus, it may be ensured that private data is actually only used in a privacy-preserving manner in order to generate individualised content, such as recommendations or a list of users with similar interests.

Typically, a number of different and variable components, such as the actual filtering techniques utilised for generating recommendations, are used within an information filtering application. With regard to trust relations, requiring each single component to remotely attest its privacy-preserving character would be rather inflexible. Therefore, a superior solution is realised by providing an environment into which these components may be deployed. In this case, only the environment itself has to remotely attest certain characteristics, independent of the actual components deployed within.

In FIDIS D14.3 “Study on the suitability of trusted computing to support privacy in business processes”, an approach for privacy-preserving information filtering based on multi-agent system technology (in which agents constitute the components, while agent platforms constitute the environment described above) will be described as an example for the suitability of trusted computing in the context of privacy-preserving information filtering.

8 Glossary

Customer relationship management	Customer relationship management (CRM) is a broad term that covers concepts used by companies to manage their relationships with customers, including the capture, storage and analysis of customer information.
Data provider	A data provider is a trustworthy place where personal and other kinds of sensitive data are stored (Pretschner, Hilty and Basin, 2006).
Data consumer	Data consumers request access to the data which is stored by data providers (Pretschner, Hilty and Basin, 2006).
Intelligent Software Agent	Intelligent Software Agent (ISA) is a software agent that uses Artificial Intelligence (AI) in the pursuit of the goals of its clients. Artificial Intelligence is the imitation of human intelligence by mechanical means. Clients, then, can reduce human workload by delegating to ISAs tasks that normally would require human-like intelligence. Delegacy for ISAs is far more absolute. ISAs have the capability to generate and implement novel rules of behaviour which human beings may never have the opportunity or desire to review. As ISAs can engage in extensive logical planning and inferencing, the relationship of trust between the client and the agent is or must be far greater, especially when the consumption of client resources is committed for reasons unexplained or multiple complex operations are actuated before human observers can react. Competency as practiced by ISAs adds higher order functionality to the mix of capabilities. In addition to communicating with their environment to collect data and actuate changes, ISAs can often analyze the information to find non-obvious or hidden patterns, extracting knowledge from raw data. Environmental modes of interaction are richer, incorporating the media of humans such as natural language text, speech, and vision. Amenability in ISAs can include self-monitoring of achievement toward client goals combined with continuous, online learning to improve performance. Adaptive mechanisms in ISAs mean that they are far less brittle to changes in environment and may actually

	improve. In addition, client responsiveness may go so far as to infer what a client wants when the client himself does not know or cannot adequately express the desired goals in definitive terms.
Information Security Management System (ISMS)	ISMS are management systems using a "good practice" approach. They cover (1) procedures (such as risk assessment or the Baseline Protection approach), (2) process models, (3) guidelines for management structures in organisations and (4) in some cases catalogues for technical security measures. Examples for "good practice" ISMS can be found in relevant standards such as ISO/IEC 27001, ISO/IEC 17799 and CobiT.
KDD	Knowledge discovery in data bases is defined as 'the non-trivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data (Fayyad, Piatetsky-Shapiro, Smyth and Uthurusamy 1996 at 6).
PPDM	Oliveira and Zaïane (2004) define PPDM as data mining methods which have to meet two targets: (1) meeting privacy requirements and (2) providing valid data mining results. These targets are in some cases – depending on the type of data mining results and the attributes in the basic data – antagonistic. In these cases the use of PPDM offers a compromise between these two targets (Meints, 2008).
Usage control	The term usage control is a generalization of access control to cover authorizations, obligations, conditions, continuity (ongoing controls), and mutability. Traditionally, access control has dealt only with authorization decisions on users' access to target resources. Obligations are requirements that have to be fulfilled by obligation subjects for allowing access. Conditions are subject and object independent environmental or system requirements that have to be satisfied for access. In today's highly dynamic, distributed environment, obligations and conditions are also crucial decision factors for richer and finer controls on usage of digital resources (Park and Sandhu, 2004).
User-centric identity management	User-centric identity management has the following properties (cf. (Josang and Pope, 2005)): • System supported identity management on the user side, resulting in improved usability.

	• Protocol flexibility, by having a personal mobile device that supports multiple authentication protocols and technologies. • Mobility, by allowing the user to use any hardware platform when accessing online services, as long as he carries his personal mobile device with him. • Backwards compatibility, by not requiring replacement of legacy identity management systems.
Service-oriented architecture	A service-oriented architecture (SOA) is a software architecture that uses loosely coupled software services to support the requirements of business processes and software users. Resources on a network in an SOA environment are made available as independent services that can be accessed without knowledge of their underlying platform implementation.

9 References

Robert Aarts, Bronislav Kavsan, and Thomas Wason: Liberty ID-FF Bindings and Profiles Specification Version: 1.2-errata-v2.0. http://www.projectliberty.org/specs/draft-libertyidff-bindings-profiles-1.2-errata-v2.0.pdf. Liberty Alliance. 2005.

Robert Aarts, Carolina Canales-Valenzuela, Scott Cantor, Frederick Hirsch, Jeff Hodges, John Kemp, John Linn, Paul Madsen, Jonathan Sergent and Greg Whitehead: Liberty ID-WSF Security Mechanisms Version: 1.2. http://www.projectliberty.org/specs/liberty-idwsf-securitymechanisms-v1.2.pdf. Liberty Alliance. 2005.

Aarts, E. and S. Marzano (eds.): The New Everyday. Views on Ambient Intelligence. Rotterdam, 010, 2003.

Rafael Accorsi: On the Relationship of Privacy and Secure Remote Logging in Dynamic Systems. In Proceedings of IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, S. Fischer-Hübner, K. Rannenberg, L. Yngström, S. Lindskog, Springer-Verlag, pp. 329—338, 2006.

Christer Andersson, Jan Camenisch, Stephen Crane, Simone Fischer-Hübner, Ronald Leenes, Siani Pearsson, John Sören Petterson, Dieter Sommer, "Trust in PRIME", Proceedings of the 5th IEEE Int. Symposium on Signal Processing and IT, December 18-21, 2005, Athens, Greece.

Rajeev Angal, Conor Cahill, Andy Feng, Gael Gourmelen, Lena Kannappan, Sampo Kellomaki, John Kemp, and Jonathan Sergent: Liberty ID-WSF Data Services Template Specification Version: v1.1. http://www.projectliberty.org/specs/liberty-idwsf-dstv1.1.pdf. Liberty Alliance. 2005.

Kristie Ball, David Lyon, David Murakami Wood, Clive Norris, and Charles Raab: A Report on the Surveillance Society: Full Report. http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance. 2006.

Carsten Bange and Heiko Schinzer: Rentablere Kundenbeziehungen durch automatisierte Analyse und Personalisierung. In Rainer Thome, Heiko Schinzer, and Martin Hepp (eds.): Electronic Commerce und Electronic Business – Mehrwert durch Integration und Automation, Vol. 3, p. 53—79, Franz Vahlen, Munich, 2005.

Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tudsik, and Michael Waidner: iKP – A Family of Secure Electronic Payment Protocols. 1st USENIX Workshop on Eletronic Commerce 1995. http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP.html. 1995.

Oliver Berthold, Hannes Federrath, and M. Köhntopp: Project 'Anonymity and Unobservability in the Internet'. In Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy 2000. p. 57—65. 2000.

J. Bohn, V. Coroama et al: Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. Ambient Intelligence. W. Weber, J. Rabaey and E. Aarts. Zurich, Springer: 5-29, 2005.

Gilles Brassard, David Chaum, and Claude Crépeau: Minimum disclosure proofs of knowledge. Journal of Computer and System Sciences Vol. 37. p. 156—189. 1988.

Stefan A. Brands: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press. 2000.

J. Buchmann, M. Ruppert, and M. Tak: FlexiPKI - Realisierung einer flexiblen Public-Key-Infrastruktur. Technical report TU Darmstadt. 1999.

L. Bygrave: Minding the Machine. Art.15 and the EC Data Protection Directive and automated profiling. Computer Law & Security Report. 17: 17-24. 2001.

Jan Camenisch and Anna Lysyanskaya: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In EUROCRYPT 2001. Vol. 2045. Springer. p. 91—118. 2001.

Jan Camenisch and Els Van Herreweghen: Design and Implementation of the idemix Anonymous Credential System. In 9th ACM Conference on Computer and Communications Security. ACM Press. p.21—30.. 2002.

Jan Camenisch and Anna Lysyanskaya: Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In Moti Yung (Hrsg.), CRYPTO 2002. Lecture Notes in Computer Science Vol. 2442. p. 61—76. Springer. 2002.

Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In SCN 2002, volume 2576 of LNCS, pages 268–289. 2002.

Jan Camenisch, Abhi Shelat, Dieter Sommer, Simone Fischer-Hübner, Marit Hansen, Henry Krasemann, Gerard Lacoste, Ronald Leenes and Jimmy Tseng: Privacy and identity management for everyone. In DIM ’05: Proceedings of the 2005 workshop on Digital identity management, New York. p. 20—27. ACM Press. 2005.

Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication. In ACM CCS (to appear), 2006.

Scott Cantor, Jeff Hodges, John Kemp, and Peter Thompson: Liberty ID-FF Architecture Overview Version: 1.2-errata-v1.0. http://www.projectliberty.org/specs/liberty-idffarch-overview-v1.2.pdf. Liberty Alliance. 2005.

Steven Carmody, Marlena Erdos, Keith Hazelton, Walter Hoehn, RL "BobMMorgan, Tom Scavo, and DavisWasley: Shibboleth Architecture Protocols and Profiles. 2005.

David Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24(2). p. 84–88. 1981.

David Chaum, Amos Fiat, and Moni Naor: Untraceable electronic cash. In CRYPTO ’88. Lecture Notes in Computer Science Vol. 403. p. 319—327. Springer. 1990.

Custers, B. (2004). The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Nijmegen, Wolf Legal Publishers.

T. Dierks und E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.1. Request for Comments 4346. 2006.

Nathan Dors: Shibboleth Architecture Technical Overview, 2005.

Dietmar Eifert: Wert von Kundenprofilen im Electronic Commerce. Electronic Commerce Vol. 28. Lohmar. Cologne. 2004.

C. Ellison, B. Frantz, B. Lamspon, R. Rivest, B. Thomas, and T. Ylonen: SPKI Certificate Theory. Internet Request for Comments 2693. Network Working Group. 1999.

EPIC and Privacy International: Privacy & Human Rights 2005. Electronic Privacy Information. 2006.

European Commission: Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities L281. p. 31—50. 1995.

European Commission: Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector (Directive on privacy and electronic communications). Official Journal of the European Communities L201. p. 37—47. 2002.

European Commission: Directive 2006/58/EC of the European Parliament and of the Council of 15th March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Official Journal of the European Communities L105. p. 54—63. 2006.

S. Farrell und R. Housley: An Internet Attribute Certificate Profile for Authorisation. Internet Request for Comments 3281. 2002.

U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy (eds.), Advances in Knowledge Discovery in Data Mining, Cambridge Mass., MIT Press 1996.

Warwick Ford and Michael S. Baum: Secure Electronic Commerce. Prentice-Hall, Inc., New Jersey. 1997.

Jason Garman: Kerberos: The Definitive Guide. O'Reilly. 2003.

German Federal Constitutional Court: Volkszählungsurteil. In Entscheidungen des Bundesverfassungsgerichts. Band 65. 1983.

German Federal Government: German Teleservices Data Protection Act. 1997.

German Federal Government: Federal Data Protection Act. 2001.

Hidehito Gomi,Makoto Hatakeyama, Shigeru Hosono, and Satoru Fujita: A delegation framework for federated identity management. New York. ACM Press. p. 94–103. 2005.

John Hagel III and John Seely Brown: Your Next IT Strategy. Harvard Business Review, p. 105—113. 2001.

Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman: Protection in operating systems. Communications of the ACM 19(8). p. 461–471. 1976.

Kurt Haubner: FiinTS V4.0 Kompendium Financial Transaction Services. SIX SIGMA EDV-Konzepte. 2004.

Harry Henderson: Privacy in the Information Age. Facts on File. New York. 1999.

Mireille Hildebrandt: Defining Profiling: A New Type of Knowledge. Profiling the European Citizen. A Cross-disciplinary Perspective. Mireille Hildebrandt and Serge Gutwirth (eds.), Springer 2008.

Mireille Hildebrandt: Technology and the End of Law. The Limits of (the Rule of) Law. E. Claes and B. Keirsbilck (eds.). to be published with Hart or Intersentia 2007.

Michael N. Huhns and Munindar P. Singh: Service-Oriented Computing: Key Concepts and Principles. IEEE Computing 49(1), p. 75—81. 2005.

International Civil Aviation Organization. Machine readable travel documents. http://www.icao.int/mrtd/Home/Index.cfm.. 2006.

Scenarios for Ambient Intelligence in 2010, Information Society Technology Advisory Group 2001, available at: http://www.cordis.lu/ist/istag-reports.htm. 2006.

The Internet of Things. Geneva, International Telecommunications Union (ITU)

Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social. Privacy Workshop September 29, 2002, University of California, Berkeley. Berkeley, available at: http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf

Uwe Jendricke and Daniela Gerd tom Markotten: Usability meets security - the Identity-Manager as your personal security assistant for the Internet. In 16th Annual Computer Security Applications Conference (ACSAC'00) 2000. 2000.

Uwe Jendricke, Michael Kreutzer, and Alf Zugenmaier: Mobile Identity Management. Technical report 178. Institute of Computer Science and Social Studies (Telematics). Workshop on Security in Ubiquitous Computing UBICOMP 2002. 2002.

Uwe Jendricke: Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement. RHOMBOS Verlag, Berlin, 2003.

Jiang, X. (2002). Safeguard Privacy in Ubiquitous Computing with Decentralized Information Spaces: Bridging the Technical and the Social. Privacy Workshop September 29, 2002, University of California, Berkeley. Berkeley, available at: http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/jiang-privacyworkshop.pdf (last visited 20th November 2006).

Audon Josang and Simon Pope: User Centric Identity Management. AusCERT Conference 2005. http://sky.fit.qut.edu.au/~josang/papers/JP2005-AusCERT.pdf, 2005.

Günter Karjoth, Matthias Schunter and Michael Waidner. Privacy-enabled Services for Enterprises In Proc. of the 13th International Conference on Database and Expert Systems Applications (DEXA'02). IEEE Computer Press, 2002

John Kemp, Paul Madsen, Jonathan Sergent, and Greg Whitehead: Liberty ID-WSF Interaction Service Specification Version v1.1. http://www.projectliberty.org/specs/liberty-idwsfinteraction-svc-v1.1.pdf. Liberty Alliance. 2005.

John Kemp, Robert Aarts, Nick Bone, David Castellanos-Zamora, Jean-Michel Crom, Lena Kannappan, Andrew Lindsay-Stewart, Kenichi Maeda, Mike Meyerstein, Alain Nochimowski, Alfredo Gonzalez, Alain Poignet, Xavier Serret, James Vanderbeek, Juliette Vittu, Alex Walter, Jonathan Sergent, Paul Madsen, Conor Cahill, John Linn, Susan Landau and Paule Sibieta: Liberty ID-FF Implementation Guidelines Version 1.2. http://www.projectliberty.org/specs/liberty-idff-guidelinesv1.2.pdf. Liberty Alliance. 2005.

J. Kohl and C. Neuman: The Kerberos Network Authentication Service (V5). Request for Comments 1510. 1993.

Markus Kohlweiss: Towards Anonymous Digital Credentials – Integrating Idemix with Access Control Products. Master thesis. University of Klagenfurt. 2003.

Thomas Kriegelstein: Entwurf und Implementierung eines Identitätsmanagement anhand eines Beispielszenarios. Master thesis, TU Dresden, 2002.

Marc Langheinrich: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. In Elgar Fleisch and Friedemann Mattern (eds.); Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. p. 329—362. Springer. 2005.

Cp. Lévy, P.: Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique. Paris, La Découverte; Hildebrandt, M. (2007). Technology and the End of Law. The Limits of (the Rule of) Law. 1990.

E. Claes and B. Keirsbilck: Liberty Alliance Project: Specifications Version 1.2. http://www.projectliberty.org/specs/liberty-20051121.zip, November 2005. last accessed at February 15th, 2006.

Thorsten Litfin and Gerd Wolfram: New Automated Checkout Systems. In Manfred Krafft and Murali K. Mantrala (eds.): Retailing in the 21st Century: Current and Future Trends., p. 143—159. Springer. 2006.

Eve Maler, Prateek Mishra, and Rob Philpott: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. 2003.

Martin Meints: 'Datenschutz durch Prozesse'. Datenschutz und Datensicherheit 2/2007. Wiesbaden 2007.

Martin Meints: Privacy Preserving Data Mining, to be published in M. Hildebrandt and S. Gutwirth (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives, Springer 2008.

Microsoft Corporation: Microsoft .NET Passport Review Guide. http://www.microsoft.com/net/services/passport/review_guide.asp. 2003.

Esther Moir: The Justice of Peace. Penguin Books. 1969.

Günter Müller and Sven Wohlgemuth (eds.): Study on Mobile Identity Management. European Commission Framework Programme Future of Identity in the Information Society (FIDIS). 2005.

K. Nielsen, R. Molich, C. Snyder and S. Farell: E-commerce user experience: Trust. Nielsen Norman Group, 2000.

Grace Ng-Kruelle, Paul A. Swatman, J. Felix Hampe and Douglas S. Rebne: The Price of Convenience: Privacy and Mobile Commerce 2002. Quarterly Journal of Electronic Commerce. p. 273-285. 2002.

Oliveira, S. R. M., Zaïane, O. R., 'Towards Standardization in Privacy-Preserving Data Mining', Proceeding of the 3rd. Workshop on Data Mining Standards (DM-SSP 2004), in conjunction with KDD 2004, Seattle, WA, USA, August, 2004. Availalbe at: http://www.cs.ualberta.ca/%7Ezaiane/postscript/dm-ssp04.pdf

Organisation for Economic Co-operation and Development: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. 1980.

Jaehong Park and Ravi Sandhu: The UCONABC usage control model. ACM Transactions on Information and System Security 7(1). p. 128–174. 2004.

John Sören Pettersson, Simone Fischer-Hübner, Mike Bergmann, "Outlining Data Track: Privacy-friendly Data Maintenance for End-users", Proceedings of the 15th International Conference on Information Systems Development (ISD 2006), Budapest, 31st August - 2nd September 2006, Springer Scientific Publishers. 2006.

John Sören Pettersson, Simone Fischer-Hübner, chapter 5.3.3 "The UI to implement functions", in: R. Leenes, S. Fischer-Hübner (Editors), PRIME Framework V2, 27 July 2006, https://www.prime-project.eu/prime_products/reports/fmwk/. 2006.

Andreas Pfitzmann and Marit Hansen: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology v0.28. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. 2006.

William Pitt: Speech on the Excise Bill.. 1765.

William Prosser: Privacy. California Law Review 48. p. 383—423. 1960.

Alexander Pretschner, Manuel Hilty and David Basin: Distributed usage control. In Communications of the ACM 49(9). Special Issue "Privacy and security in highly dynamic systems". p. 39—44. ACM Press. 2006.

Kai Rannenberg, Andreas Pfitzmann, and Günter Müller: IT Security and Multilateral Security. In: Multilateral Security in Communications - Technology, Infrastructure, Economy. P. 21—29. Addison-Wesley-Longman. 1999.

R. L. Rivest, A. Shamir, and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2). p. 120–126. 1978.

Alexander Roßnagel: Moderinisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung. Multimedia und Recht 8(2). 2005.

Stefan Sackmann and Jens Strüker: Electronic Commerce Enquête 2005 – 10 Jahre Electronic Commerce: Eine stille Revolution in deutschen Unternehmen. Technical Report, Institute of Computer Science and Social Studies (Telematics), Freiburg I.Br., 2005.

Stefan Sackmann, Jens Strücker, and Rafael Accorsi: Personalization in Privacy-Aware Highly Dynamic Systems. Communications of the ACM, Vol. 49(9), p. 32—38. 2006.

Jerry H. Saltzer and Mike D. Schroeder: The protection of information in computer systems. In proceedings of the IEEE 63(9). p. 1278—1308. 1975.

F. Schauer: Profiles Probabilities and Stereotypes. Cambridge, Massachusetts London, England, Belknap Press of Harvard University Press. 2003.

Roland E. Schmid, Volker Bach, and Hubert Österle: Mit Customer Relationship Management zum Prozessportal, Springer, 2000.

W. Schreurs and M. Hildebrandt: Legal Issues. Report on the Actual and Possible Profiling Techniques in the Field of Ambient Intelligence. W. Schreurs, M. Hildebrandt, M. Gasson and K. Warwick. Brussels, FIDIS deliverable 7.3, available at www.fidis.net: 36-59. 2005.

W. Schreurs, M. Hildebrandt et al.: Cogitas ergo sum: The role of data protection law and non-discrimination law in group profiling in the private sphere. Profiling the European Citizen: Cross-Disciplinary Perspectives. Mireille Hildebrandt and Serge Gutwirth (eds.), Springer, 2008.

Igor Sedov, Marc Haase, Clemens Cap, and Dirk Timmermann: Hardware Security Concept for Spontaneous Network Integration of Mobile Devices. In Proceedings of the International Workshop "Innovative Internet Computing Systems". Ilmenau. 2001.

Shyong K. “Tony” Lam, Dan Frankowksi, and John Riedl: Do You Trust Your Recommendation? An Exploration of Security and Privacy Issues in Recommender Systems. In Proceedings of Emerging Trends in Information and Communication Security (ETRICS) 2006. Lecture Notes of Computer Science. Vol. 2995. p. 14—29. Springer. 2006.

Robert Ellis Smith: The law of privacy in a nutshell. Privacy Journal 19(6). P. 50—51. 1993.

Daniel J. Solove: A Taxonomy of Privacy. University of Pennsylvania Law Review 154(3), p. 477—564, 2006.

Daniel J. Solove: The Digital Person: Technology and Privacy in the Information Age. New York University Press. 2006.

Jens Strüker and Stefan Sackmann: New Forms of Customer Communication: Concepts and Pilot Projects. In Proceedings of the 10th Americas Conference on Information Systems (AMCIS ’04) USA. 2004.

United Nations: The Universal Declaration of Human Rights. http://www.unhchr.ch/udhr/index.htm. 1948.

Carolina Canales Venezuela, Garry Ellison, Jeff Hodges, Sampo Kellomäki, John Kemp, John Linn, and Peter Thompson: Liberty ID-WSF Security and Privacy Overview Version: 1.0. http://www.projectliberty.org/specs/liberty-idwsf-securityprivacy-overview-v1.0.pdf. Liberty Alliance. 2005.

Von Welch, Ian Foster, Carl Kesselmann, Olle Mulmo, Laura Pearlman, Steven Tuecke, Jarek Gawor, Sam Medder, and Frank Siebenlist: X.509 Proxy Certificates for Dynamic Delegation. In 3rd Annual PKI R&D Workshop. 2004.

Samuel D. Warren and Louis D. Brandeis: The Right to Privacy. Harvard Law Review 193(4). 1890.

Alan F. Westin: Privacy and Freedom. Atheneum. New York. 1967.

Sven Wohlgemuth, Uwe Jendricke, Daniela Gerd tom Markotten, Felix Dorner, and Günter Müller: Sicherheit und Benutzbarkeit durch Identitätsmanagement. In D. Spath and K. Haases (eds.): Tagungsband zum doIT Software-Forschungstag 2003, Aktuelle Trends in der Softwareforschung, Stuttgart, p. 241—260, IRB Verlag, 2004.

Angelos Yannopoulos, Vassiliki Andronikou and Theodora Varvarigou, 'Behavioural Profiling and Ambient Intelligence', in: Mireille Hildebrandt and Serge Gutwirth (eds.) Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer 2008.

W. Yeong, T. Howes, and S. Kille: Lightweight Directory Access Protocol. Internet Request for Comments 1777. 1995.

Alf Zugenmaier: Anonymity for Users of Mobile Devices through Location Adressing. RHOMBOS-Verlag. 2003.

Zarsky, T. Z.: "Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion." Yale Journal of Law & Technology 5 (4): 17-47, 2002-2003.