

**Identity Management Systems (IMS):  
Identification and Comparison Study**

**Independent Centre for Privacy Protection (ICPP) /  
Unabhängiges Landeszentrum für Datenschutz (ULD)  
Schleswig-Holstein**

**and**

**Studio Notarile Genghini (SNG)**

**2003-09-07**

**Contract N°19960-2002-10 F1ED SEV DE.**



## EXECUTIVE SUMMARY

Identity management is one of the most far-reaching and promising topics for modern society, but barely analysed so far. Administering and controlling identities will presumably become a task which requires technological support. Identity Management Systems (IMS) will provide such technological assistance for managing identities. A holistic all-purpose tool for identity management is still a mere vision. In the current discussion of industry and academia, specific solutions of Identity Management Systems are elaborated which deal with the following **core facets**:

- Everybody in information society possesses many accounts (so-called digital identities) where authentication data such as passwords or PINs have to be memorised. As a unique and universal ID concept is far from being implemented – not only because of privacy obstacles – the amount of **digital identities** per person will even increase in the next years. Users need convenient support for managing these identities and the corresponding authentication methods.
- Users also need convenient support for situations where they are addressed by other people or even machines. **Reachability** management could put users in a better position to handle their contacts by providing an intelligent filter mechanism, e.g., to prevent spam e-mail or unsolicited phone calls.
- Today's digital networks do not ensure **authenticity** and render an **identity theft** rather easily. Systems which support methods for authentication, integrity and non-repudiation such as digital signatures can prevent unnoticed unauthorised usage of digital identities.
- Users leave data trails by using digital networks – mostly without their knowledge and without any possibility to prevent those trails. Instead each user should be empowered to control which parties can link different occurrences of one's personal data in order to estimate how much they know about oneself. This demand can be derived from the right to informational self-determination. Methods to support users in asserting this right are being developed, e.g., for providing **anonymity** or **pseudonymity**.
- **Organisations manage personal data** of their employees and are in need of quick methods for creating, modifying and deleting work accounts. Additionally to this internal management of members, organisations strive for administration of their client data, using e.g., profiling techniques.

Regarding these aspects, this study focuses on the **user-controlled management of own identities** rather than describing systems, which only do user profiling without offering the individual a possibility to manage those data. These types of self-called "Identity Management Systems" are found quite often in today's business, but in contrast to the user-controlled Identity Management Systems they concentrate on business processes rather than comprising the user's point of view. With our notion of IMS, putting the user in the centre, but nevertheless discussing possible implications also for organisations of different kinds, we take into account, that IMS in fact create a new paradigm in the sociological, legal and technological realm.

The study "Identity Management Systems (IMS): Identification and Comparison" is built on **four pillars**:

1. **Basis of and requirements** for Identity Management Systems, which are elaborated from sources of academic literature and business information;
2. **Usage scenarios**, which show the practical relevance and additional requirements of IMS in various contexts;
3. Analysis of presently available **Identity Management Applications**;

4. **Survey** on expectations on Identity Management Systems, which was conducted among experts world-wide.

It is important to point out that technologically supported identity management affects the whole social evolution. In order to correlate the evaluation of applications and the reflection on social impacts of IMS, we made the important distinction between "**Identity Management System**" (IMS) and "**Identity Management Application**" (IMA): We define the term "Identity Management System" as an infrastructure, in which "Identity Management Applications" as components are co-ordinated. Identity Management Applications are tools for individuals to manage their socially relevant communications, which can be installed, configured and operated at the user's and/or a server's side.

### **1<sup>st</sup> Pillar: How to construct identity**

The "identity" of an individual in the form of a person can be described as mostly socially formed. Henceforth, it becomes necessary in order to understand the complexity of identities to distinguish the **social contexts** in which persons navigate and in which some of their partial identities, bundles of attributes of their complete identity, become relevant. From the standpoint of sociology, the main types of social systems need to be discussed as specialised forms which are operating along the difference of "I" and "Me" and the difference of "role making" and "role taking". Identity management then means recognition of situations and their valuation as "applicable to one self" (role taking) or forming them (role making). IMS should assist users to correctly identify social situations and their relevant addressing options. The perspective of future information society is: No communication without the assistance of an IMA.

Switching to the **legal perspective**, identity management is not explicated by legislation as such. Identity from a legal perspective has a dual function: identification of subjects and reference point for rights and obligations. Nonetheless legislation provides some (in most cases) constitutionally protected rights to individuals, that allow them to change some aspects of their identity, even if such changes are in conflict with uniqueness and identifiability of subjects. In this sense one could point to well-known, conventional rights like "right to a name", "right to change name", "right to have a pseudonym", "right to move and to change domicile", "right to dress and decide the personal outlook", "right to be left alone (privacy protection) and right to anonymity", "right to change gender" and "right of honour". The legal perspective also includes the liability of the user and giving evidence.

A **technically supported identity management** through Identity Management Applications respectively Identity Management Systems has to empower the user to realise the right to communicational self-determination. For this purpose it should recognise different kinds of social situations and assess them with regards to their relevance, functionality and their security and privacy risk in order to find an adequate role making and role taking. Pseudonyms and credentials, i.e., convertible authorisations, are the core mechanisms for the handling or the representation of identities. The IMA should provide functions for context detection and support the user in choosing the appropriate pseudonym. A log function for all transactions of the IMA should give valuable input to the context detection module and inform the user about past transactions.

The **analysis** of identity management in the socio-psychological, legal, and technological contexts demonstrates:

- Role management, which has been handled intuitively by people so far, will become explicit.
- The current regulatory framework in the EU offers many degrees of freedom in pseudonym handling without inevitably losing assurance in legally binding transactions.

- Although technological concepts of multi-purpose privacy-enhancing identity management are already about 20 years old, they have only been partially implemented, yet.

All these findings prepare the ground for an effective identity management in both the off-line and the on-line world.

## 2<sup>nd</sup> Pillar: Usage Scenarios

We have analysed 18 usage scenarios which demonstrate typical workflows in different social contexts and which are relevant to a big population group. These scenarios show the practical relevance of identity management and identify requirements for IMS/IMA. We started with some basic identity-related scenarios like identity theft and data trails to give some ideas on the general problems in today's digital networks. These lead to **general scenarios** of multi-purpose IMA as PDAs, the identity protector concept, and the task assignment scenario to prepare the ground for more specific scenarios. One main part of the study was the examination of more concrete scenarios like **e-Commerce** (e-Shopping, e-Auction, e-Banking), **e-Government** (tax declaration, inquiry), **e-Court** (civil action, on-line mediation, criminal proceedings), **e-Voting**, **e-Health**, and some miscellaneous scenarios like **e-Science** (review process), **e-Notary** (**e-Witness**), and Location Based Services.

In each scenario firstly the current workflow for handling the concerned task is described. Then the role of identity management is elaborated, giving the benefits and explaining a possible integration – considering necessary **modifications in the traditional workflow** – of identity management functionality. We derived requirements from each scenario, focusing on the specifics of each scenario where we explicitly concentrate on the demands for identity management functionality.

The analysis of the scenarios results in the following:

- Most typical applications consist of logically separated **pseudonym domains** where any linkability of the user's personal actions can be avoided in order to provide maximum privacy. This may be achieved by separating distinct transactions, e.g., by using different pseudonyms for usage, payment, and delivery of goods. The concept of pseudonym domains can be used in all kinds of scenarios as a structuring method which shows the possibilities for identity management support with respect to pseudonyms.
- When designing and implementing identity management support for a workflow, the appropriate **types of pseudonyms** have to be used. Typical pseudonym properties may be, e.g., addressability by other parties, possibility of re-use, e.g., in order to built a reputation, limitation of validity, transferability to other persons, or the possibility to reveal the identity of the pseudonym holder by other parties under specific circumstances.
- There are scenarios where identity management and the detachment of pseudonym domains are already practised today (e.g., review processes). For some scenarios identity management could make the workflow more effective and could help to avoid media conversions while raising the **privacy level** (like tax declaration, e-Court, e-Voting). The implementation of some of the scenarios (e.g., tax declaration, e-Court) would require the prior adaption of national regulations.

## 3<sup>rd</sup> Pillar: Evaluating Identity Management Applications

We have sighted the presently known products for identity management, compiled a **list of the main products and prototypes** (88 entries), and tested some of them. Selection criteria for test candidates were whether the products are popular or setting trends, whether they were mentioned by the experts in the survey or whether they cover the aspects of the introduced so-called "operational areas", i.e., access management, form filling, automatic choice of identity, pseudonym management, and reachability management.

The **evaluated products** comprise Mozilla 1.4 Navigator, Microsoft .NET Passport, Liberty Alliance Project, Novell Digitalme, Yodlee, Microsoft Outlook Express 6 SP1, and CookieCooker. Additionally some **trend setting** products or prototypes were shortly described: ATUS, DRIM, Sun One, Digital Identity, Open Privacy, IBM WS-Security, and American Express Private Payments.

These products demonstrate the bandwidth of what current technologically supported identity management could mean. We have evaluated the Identity Management Applications according to requirements that are analogously used for describing consumer requirements in relation to ICT standardisation. These requirements were substantiated in form of a **grid of attributes** which comprises functionality, usability, security, privacy, law enforcement, trustworthiness, affordability, and interoperability.

In general we can distinguish between **centralised identity** and **federated identity**: Centralised identities are provided by a central IMS provider which acts like a single gateway for the user's management of identities. Federated identities have multiple IMS providers. As there is no concentration of personal data outside the users' scope, users have more control over what personal data they share with whom. Federated identity management puts bigger responsibilities on the user and can mean more effort in user support. In contrast to that, centralised identity management is easier and cheaper to maintain, but the single point of control also means a single point of failure and an attractive target for attackers.

The evaluation of Identity Management Applications according to the grid of attributes results in the following:

- The available products and prototypes vary in **functionality range and maturity**. This indicates that the business models for IMA and the academic perception of this topic have not yet been solidified, but are still pliable.
- None of the evaluated products meets all elaborated criteria. There are especially significant **deficiencies** regarding privacy, security, and liability functionality. Applications which try to address such functionalities reveal usability problems.
- Many products rely on the centralised identity model which offers less control by the user, but is easier to implement and to maintain. It will be a **question of trust** whether users might agree to the involvement of central identity management providers or prefer to manage their identities on their own.

The building blocks for a multi-purpose Identity Management System, that will take security and privacy criteria into account, seem to exist at least on a conceptual level. Still there are some **open research questions** – not only in the technological, but also in the legal and socio-economic fields.

The overview of Identity Management Applications reveals an advantage of the US in the field of distributed products, whereas the European Union scores especially regarding innovative identity management concepts, fitting into the legal and cultural EU framework. The study highlights **EU capacity** to transform those concepts into marketable solutions. Privacy seals could help to tag those IMA which implement privacy-enhancing concepts and are compliant to law, e.g., the European Data Protection Directive.

#### 4<sup>th</sup> Pillar: What do experts think on IMS?

During this study a survey on IMS was conducted. The developed questionnaire was answered by **89 experts world-wide** from research, business, administration, and data protection authorities. Most of the experts who answered came from a European background. Nearly half of the experts were researchers at universities or companies. In the perception of most of the

answering experts, Identity Management Systems are rather the subject of a predominantly technologically oriented research than already real products. IMS is still a research topic where concepts or visions are being discussed. However, a few of the experts understand a privacy-reflecting dealing with standard communication software as technology-based identity management. An extensively fixed paradigm of what makes and includes an IMS has obviously not yet gained general acceptance.

The main results of the survey on Identity Management Systems (in the meaning of "Applications") show:

- So far there is no generally accepted paradigm of IMS. Nevertheless, experts predict a good marketability of IMS after a period of **10 years'** time.
- As the main obstacle to proliferation of Identity Management Systems we have identified not pure technology factors like, e.g., insufficient security, but **socially related factors** such as insufficient usability and slow standardisation.
- Privacy protection, security, and usability consistently receive the highest scores from the experts as **essential functions** of IMS.

### Conclusion

This study shows that a user-controllable IMS is plausible and probable from a sociological perspective, already possible as of today on a basis of Europe-wide regulations, and technically presumably copeable. Considering the use of IMS in fields of operation such as e-commerce and e-government by means of future scenarios, we conclude that many workflows would work more effectively based on IMS while integrating a better privacy level than up to now. The evaluation of currently available applications and studies of concepts respectively prototypes of identity management anticipates the path which technological development will pursue. Thereby experts expect complicated usability of Identity Management Applications, an inadequate level of computer security and privacy, and also lengthy standardisation processes as main bottlenecks for developing a society-wide Identity Management System.



## PREFACE

In the summer 2002 the Institute for Prospective Technological Studies (IPTS), Joint Research Centre Seville, has been published an invitation to tender on Identity Management Systems (Tender No J04/02/2002). The objective of the study is the evaluation of existing and emerging Identity Management Systems and the deduction of recommendations for European policy makers.

This study "Identity Management Systems (IMS): Comparison and Identification" has been elaborated by a consortium consisting of the Independent Centre for Privacy Protection (Unabhängiges Landeszentrum für Datenschutz) Schleswig-Holstein, Kiel, Germany, and Studio Notarile Genghini, Milano, Italy. Both consortium partners have been working in the field of identity management for several years. The consortium therefore commands broad knowledge and in-depth expertise on legal, technical, socio-cultural and economical aspects and implications of identity management.

The identity of a person comprises many partial identities which represent the person in specific contexts or roles. In short, identity management means managing the various partial identities. There is a widespread sense of inadequacy of the utilisation and management of our identities on open networks.

- Considering these identities there is a question not only of proper identification and authentication, but also of presentation.
- In their substance and interpretation, partial identities of one person are predominantly determined by third parties, with significant implications for privacy, freedom and self-determination: The social aspect of identity becomes tapered in the reduction of humans to marketing-driven profiles.

Because of this, the present study did not restrict itself to a description of existing solutions in order to propose generic improvements. In our understanding such an approach would have been limiting and it would fall short in describing solutions for shortcomings in handling and management of identities, as perceived by many Internet users. Thereby, we hope to avoid any implicit a-priori assumptions.

Also we appreciate the work which has been done in areas which are related to general or specific identity management approaches, requirements, mechanisms, and trends, e.g., in the fields of national identity cards, identity proof, authentication<sup>1</sup>, biometrics<sup>2</sup>, cryptology, security, privacy or privacy-enhancing technologies<sup>3</sup>, anonymity<sup>4</sup>, trust<sup>5</sup>, e-commerce, citizens' rights<sup>6</sup>, etc. This study does not rewrite the findings in those fields, but rather takes them as a solid basis and builds on top, developing the approach to Identity Management Systems and Applications on a higher level. As IMS begin to evolve and comprise the capability of bringing forward information society, this study includes a visionary outlook. However, the synthesis of this study keeps in touch with reality, establishing a link between theory and practise, in particular by use scenarios.

<sup>1</sup> [Cf. Kent/Millett 2003].

<sup>2</sup> [Cf. The Freedonia Group, Inc.: Biometrics & Electronic Access Control Systems to 2005 – Market Size, Market Share and Demand Forecast; Nov. 2001; United States; [http://freedonia.ecnext.com/free-scripts/comsite2.pl?page=description&src\\_id=0001&study\\_id=1503](http://freedonia.ecnext.com/free-scripts/comsite2.pl?page=description&src_id=0001&study_id=1503).

<sup>3</sup> [Cf. van Rossum/Gardeniers/Borking et al. 1995].

<sup>4</sup> E.g., Study from American Association for the Advancement of Science, cf. Al Teich, Mark S. Frankel, Rob Kling, Ya-Ching Lee: Anonymous Communication Policies on the Internet: Results and Recommendations of the AAAS Conference; The Information Society; Vol. 15, No. 2; 71-77; 1999; <http://www.indiana.edu/~tisj/>.

<sup>5</sup> E.g., the following joint research study: Studio Archetype/Sapient and Cheskin: eCommerce Trust Study; January 1999; <http://www.cheskin.com/p/ar.asp?mlid=7&arid=40&art=0&isu=1>.

<sup>6</sup> [Cf. LIBE 2003].

## ABSTRACT OF CHAPTERS

This study draws requirements and mechanisms out of an analysis of the sociological, legal and technical dimensions of identity (Chapters 1.1, 1.2 and 1.3) combining such findings with the technical properties of technologies that can be (Chapter 2) or are already (Chapter 3) used for managing our identities.

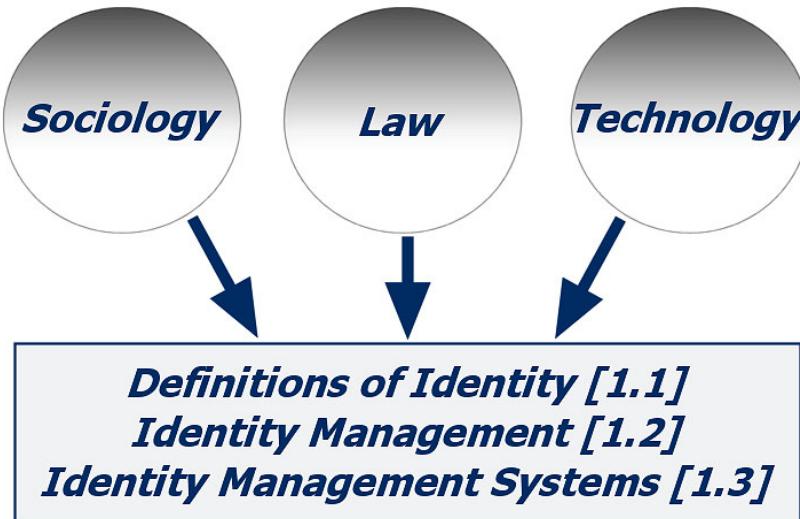


Figure 1: Overview over Chapter 1

Therefore, Chapter 1 has been devoted to the discovery and justification of existing definitions of:

- Identity: from a sociological perspective, in Chapter 1.1.1; from a legal perspective, in Chapter 1.1.2; from a technical perspective in Chapter 1.2.3.
- Identity Management (IM): from a sociological perspective, in Chapter 1.2.1; from a legal perspective, in Chapter 1.2.2; from a technical perspective in Chapter 1.2.3. In Chapter 2.1 a series of scenarios are presented that highlight how legislation can reconcile and regulate uniqueness and multiplicity of human identity.
- Identity Management System (IMS) and Identity Management Application (IMA): from a sociological perspective, in Chapter 1.3.1; from a legal perspective, in Chapter 1.3.2; from a technical perspective in Chapter 1.3.3.

Chapter 1 highlights that legislation provides increasing rights to freedom and self-determination that allow and even protect the right to manage the own identity, although there is no explicit right to identity management, yet. Therefore the definitions and concepts of IMS and of IMA have to be considered not only in a technical environment, but also from a legal and sociological perspective. It is the same technical environment that poses actually the greatest threat to a free, self-determined and conscious choice (and management) of one's identity. In Chapter 1.4, we describe the actors of IMS, followed by clarifying some terminology related to the study (Chapter 1.5).

The fundamental difference between profiling and IMA and IMS has been clarified in Chapter 1, pointing out that profiling is in functional terms the exact opposite of IM, because it shifts the control on identity to third parties with reducing control and so freedom of choice. In Chapter 1 also the difference between IMA and IMS is defined.

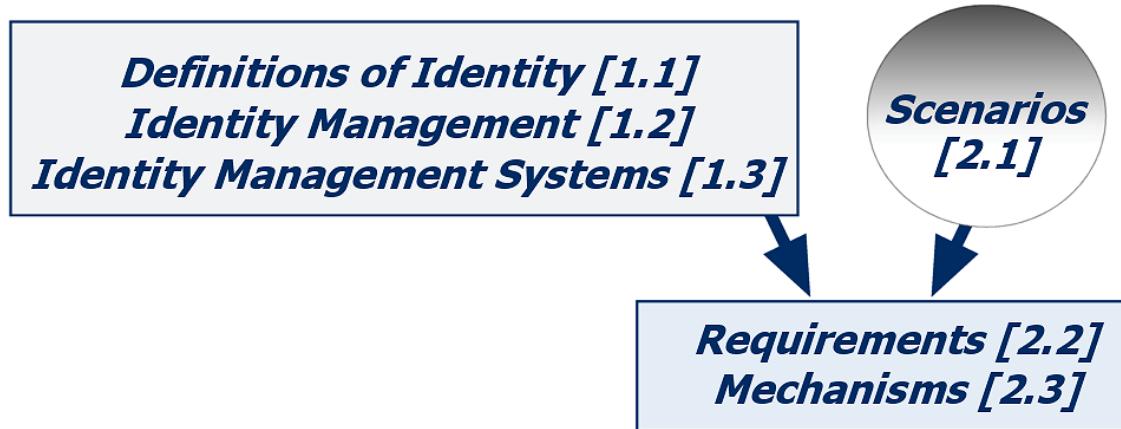


Figure 2: Chapters influencing Chapter 2

Chapter 2 elaborates usage scenarios for identity management and derives requirements and mechanisms. In Chapter 2.1, we describe possible usage environment of IMA and IMS. In Chapters 2.2 and 2.3 a full set of requirements and mechanisms are provided, which have been defined in consideration of the usage scenarios set in Chapter 2.1 and of the definitions of IM and IMS and of IMA provided by Chapters 1.2 and 1.3.

In Chapter 3 the results of a wide market research of systems, solutions and applications that are actually involved in managing to some extent identities or designed to do it are being analysed. Almost none of the retrieved solutions fully fits the definitions of IMS or IMA conditions.

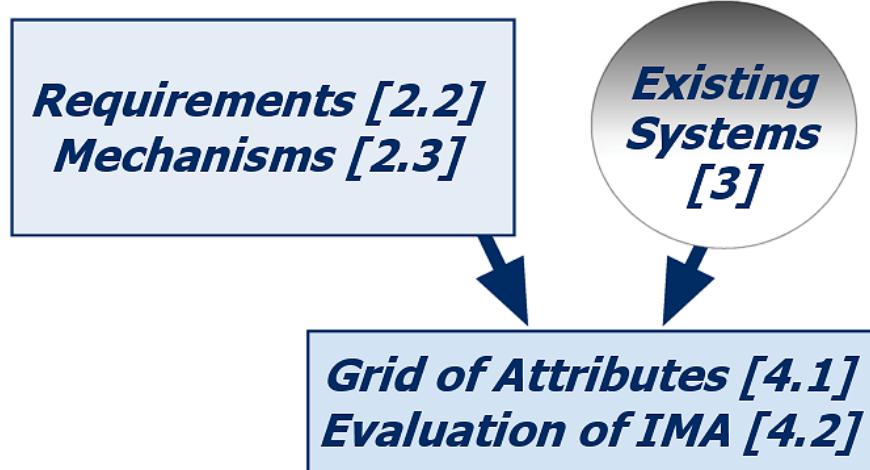
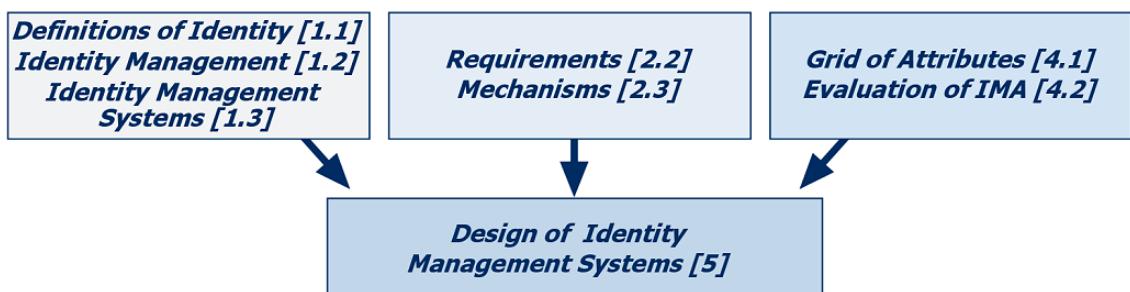


Figure 3: Chapters influencing Chapter 4

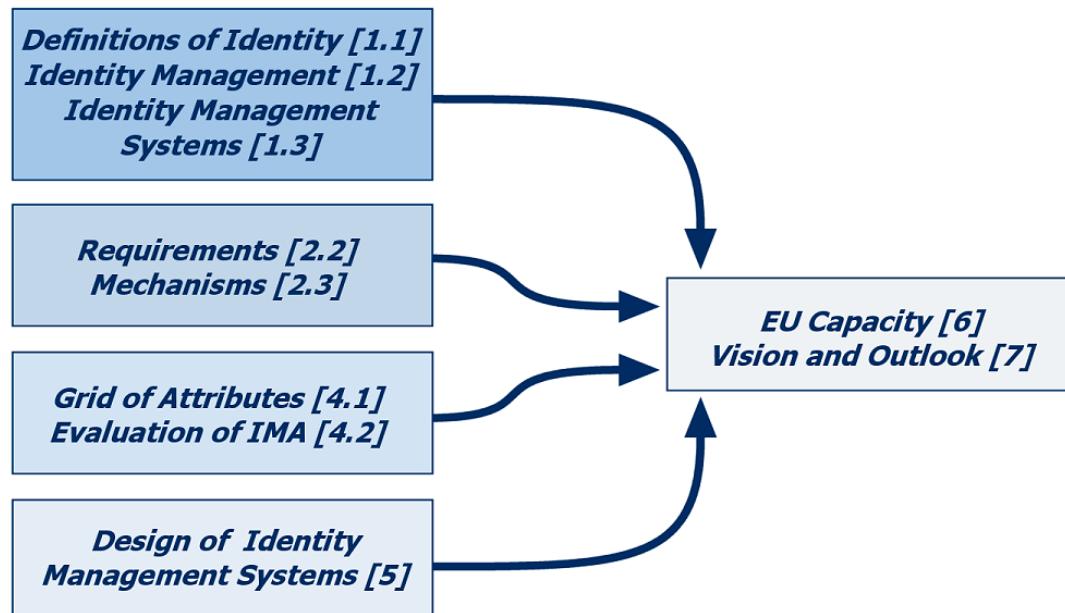
Chapter 4 compares the main systems retrieved in Chapter 3 using a benchmark (grid of attributes), that has been set utilising the definitions and information provided in particular by Chapters 1.2 (definition of IM), 1.3 (definition of IMS), 2.1 (usage scenarios for IMS and IMA) and 2.2 and 2.3 (requirements and mechanisms for IMA and IMS). It is interesting to note that although the same technology that today reduces the freedom of choice and self-expression is capable of enhancing the individual's control of his or her identity. Chapter 4 shows that this is not a consequence of the technology itself, but of the way it is implemented: it is a problem of business models and not something that is dictated by the needs or the restraints of the technology so far available.



**Figure 4: Chapters influencing Chapter 5**

Building on these results, Chapter 5 designs a different way of integrating the existing technologies in IMA and IMS according to the requirements and mechanisms set in Chapters 2.2 and 2.3 in a way that is respectful of the individual needs and rights that have been outlined in Chapters 1.1 and 1.2.

In Chapter 6, we describe the EU capacity in the field of identity management and point out possible steps to promote the development of IMS or IMA which fulfil the elaborated criteria. This could lead to a positive impact on the existing business models, enhancing at the same time user empowerment and business opportunities.



**Figure 5: Chapters influencing Chapters 6 and 7**

In Chapter 7, we indicate a possible long-term roadmap and alternative long-term scenarios, setting the scene for some visionary outlook.

Chapter 8 presents the questionnaire and the results of surveying several experts on identity management while elaborating this study.

A comprehensive list of references and a glossary complement the study. Moreover, additional material is listed in the Annex:

- Details on the questionnaire, which results have been shown in Chapter 8;
- Information on the roadmap on IMS, which was produced by the RAPID project and is mentioned in Chapter 7;
- A comparison of three IMA by the Article 29 Working Party, as quoted in Chapters 4, 5, and 6; and
- Legal material, in particular on electronic signatures and on pseudonymity.

## **ACKNOWLEDGEMENTS**

The author team, consisting of Marit Hansen, Henry Krasemann, Christian Krause, and Martin Rost from the Independent Centre for Privacy Protection Schleswig-Holstein, Germany, and of Dr. Riccardo Genghini from Studio Notarile Genghini, Italy, thanks all individuals who contributed to the work of this study. We are grateful to the experts who answered the questionnaire on Identity Management Systems. Thanks are also due to the IPTS who sponsored and accompanied the study. Furthermore, the IPTS team with Laurent Beslay, Clara Centeno, Ioannis Maghiros, and Carlos Rodriguez provided valuable input. We thank the following people especially for background research, intense discussions, intelligent translation support and proof-reading and their manifold help and advice: Dr. Helmut Bäumler, Dr. Peter Berlich, Sebastian Clauß, Martin Jöns, Thomas Kriegelstein, Cristina Lomazzi, Dr. Thomas Petri, Dr. Daniela Rocca, Michael Schack, Dr. Marietta Gräfin Strasoldo, Dr. Thilo Weichert, Markus Wiese.



---

# CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>I</b>
<b>PREFACE.....</b>	<b>VII</b>
<b>ABSTRACT OF CHAPTERS.....</b>	<b>VIII</b>
<b>ACKNOWLEDGEMENTS.....</b>	<b>XI</b>
<b>1 [CHAPTER A: DEFINITION OF IDENTITY MANAGEMENT SYSTEMS] .....</b>	<b>1</b>
1.1 Definition of Identity.....	1
1.1.1 Identity from the Sociological Perspective .....	1
1.1.2 Identity from the Legal Perspective .....	7
1.1.3 Identity from the Technical Perspective.....	18
1.2 Definition of Identity Management.....	19
1.2.1 Identity Management from the Sociological Perspective.....	19
1.2.2 Identity Management from the Legal Perspective .....	20
1.2.3 Identity Management from the Technical Perspective.....	28
1.3 Definition of Identity Management System .....	29
1.3.1 IMS from the Sociological Perspective.....	29
1.3.2 IMS from the Legal Perspective .....	30
1.3.3 IMS from the Technical Perspective.....	30
1.3.4 Multi-purpose Identity Management Application.....	32
1.4 Actors.....	33
1.4.1 Users .....	35
1.4.2 Service Providers .....	36
1.4.3 IMS Providers .....	37
1.5 Definition of Related Terms.....	37
1.5.1 Definition of Anonymity.....	37
1.5.2 Definition of Pseudonymity / Pseudonym .....	37
1.5.3 Definition of Unlinkability.....	38
1.6 Summary .....	39
<b>2 [CHAPTER B: BASIC REQUIREMENTS AND MECHANISMS] .....</b>	<b>41</b>
2.1 Scenarios for Identity Management .....	41
2.1.1 General Identity-Related Scenarios.....	41
2.1.2 General Scenarios .....	44
2.1.3 E-Commerce .....	49
2.1.4 E-Government, E-Court and E-Democracy .....	57
2.1.5 E-Health .....	66
2.1.6 Miscellaneous .....	68
2.1.7 Conclusion .....	73
2.2 Main Requirements .....	75
2.2.1 Functionality .....	75
2.2.2 Usability .....	76
2.2.3 Security .....	77
2.2.4 Privacy .....	78
2.2.5 Law Enforcement.....	79
2.2.6 Trustworthiness.....	81
2.2.7 Affordability .....	81
2.2.8 Interoperability.....	81
2.3 Mechanisms .....	81
2.3.1 Communication-Independent Handling and Representation of Identities.....	83
2.3.2 Pseudonyms with Specific Properties .....	84
2.3.3 Credentials .....	87
2.3.4 Identity Recovery.....	89
2.3.5 Interfaces for Communication and Import/Export .....	89
2.3.6 History Management.....	89
2.3.7 Privacy Control Functionality.....	89
2.3.8 Context Detection .....	90
2.3.9 Rule Handling .....	90
2.3.10 Handling of Identities in the Communication .....	90

---

2.3.11	Infrastructural Environment Requirements: Anonymous Communication Network and Secure Systems .....	90
2.3.12	Mechanisms for Trustworthiness .....	91
2.3.13	IMS Mechanisms with Respect to Co-operating Parties.....	92
2.4	Summary .....	94
<b>3</b>	<b>[CHAPTER C: LIST OF EXISTING SYSTEMS] .....</b>	<b>95</b>
3.1	Criteria .....	95
3.1.1	Basics .....	95
3.1.2	Operational Areas .....	95
3.1.3	Miscellaneous .....	96
3.2	List of IMA Ordered by Availability and Nations .....	98
3.3	Alphabetic List of IMA .....	101
3.4	Summary .....	103
<b>4</b>	<b>[CHAPTER D: FULL SCALE COMPARISON OF THE MAIN SYSTEMS] .....</b>	<b>105</b>
4.1	Grid of Attributes .....	105
4.1.1	Overview .....	105
4.1.2	Functionality .....	106
4.1.3	Categories .....	107
4.1.4	Platform and Environment .....	111
4.2	Evaluation of Identity Management Applications.....	112
4.2.1	Mozilla 1.4 Navigator .....	114
4.2.2	Microsoft .NET Passport.....	125
4.2.3	Liberty Alliance Project .....	137
4.2.4	Novell Digitalme.....	150
4.2.5	Yodlee .....	160
4.2.6	Microsoft Outlook Express 6 SP1 .....	168
4.2.7	CookieCooker .....	177
4.2.8	Other Interesting Approaches .....	188
4.2.9	Summary .....	198
<b>5</b>	<b>[CHAPTER E: DESIGN OF AN IDENTITY MANAGEMENT SYSTEM].....</b>	<b>201</b>
5.1	Basic Architectures .....	201
5.2	Different Zones of Trust.....	202
5.3	Identity Handling .....	203
5.3.1	Centralised vs. Federated Identity.....	203
5.3.2	Self-Authentication vs. External Authentication.....	204
5.3.3	Number of Identities per Person .....	204
5.3.4	Global Identity vs. Partial Identity .....	204
5.3.5	Transfer of Credentials.....	204
5.4	A Common System Design: Infomediaries .....	205
5.5	A Privacy-Enhancing IMS Architecture .....	205
5.6	Summary .....	206
<b>6</b>	<b>[CHAPTER F: EU CAPACITY].....</b>	<b>207</b>
6.1	EU Capacity .....	207
6.1.1	Developing the Regulatory Frame .....	207
6.1.2	Strengthening Leadership in Specific Technologies .....	208
6.1.3	Cultivating Market Niches .....	209
6.1.4	Funding .....	210
6.1.5	Standardising Identity Management.....	210
6.1.6	Building Infrastructures .....	212
6.1.7	Gaining Awareness .....	212
6.1.8	Exporting EU Know-how .....	212
6.2	Summary .....	213
<b>7</b>	<b>[CHAPTER G: VISION AND OUTLOOK] .....</b>	<b>214</b>
7.1	Roadmap .....	214
7.1.1	RAPID – An Existing Roadmap on Privacy and Identity Management .....	214
7.1.2	An Approach to an IMS Roadmap .....	215
7.2	Outlook .....	222
7.3	Summary .....	224
<b>8</b>	<b>[CHAPTER H: QUESTIONNAIRE].....</b>	<b>227</b>
8.1	Background of the Responding Experts .....	227

---

---

8.2	Estimations on Identity Management.....	231
8.2.1	Applications for Identity Management .....	231
8.2.2	Essential Functions of an Identity Management System.....	232
8.2.3	Marketability of an Identity Management System .....	234
8.2.4	Bottlenecks Regarding Mass Adoption of Identity Management Systems .....	235
8.2.5	Important Aspects of an Identity Management System for Use on a Grand Scale within Society .....	236
8.2.6	Degree of Centralisation with Respect to the Administration of Personal Data .....	237
8.2.7	Socio-Psychological Consequences of Usage of an IMS.....	238
8.2.8	Estimated Effect on Law Enforcement .....	240
8.3	Summary .....	240
<b>REFERENCES.....</b>		<b>242</b>
<b>GLOSSARY.....</b>		<b>253</b>
<b>ANNEXES.....</b>		<b>255</b>
<b>1</b>	<b>QUESTIONNAIRE .....</b>	<b>255</b>
1.1	Form Letter and Questionnaire .....	255
1.2	Results.....	262
1.3	Some Methodically Notes .....	282
1.3.1	Return Quota .....	282
1.3.2	Methodical Inadequacies and Mistakes.....	283
1.3.3	Generally Remarks on the Questionnaire (V56) .....	284
<b>2</b>	<b>RAPID'S ROADMAP ON PRIVACY AND IDENTITY MANAGEMENT .....</b>	<b>285</b>
2.1	Introduction.....	285
2.2	Research Plan PET in Enterprise (R-PE) .....	285
2.3	Research Plan PET in Infrastructure (R-PI) .....	287
2.4	Research Plan Multiple and Dependable Identity Management (R-MIM).....	287
2.5	Research Plan Socio-Economic (R-SE) .....	288
2.6	Research Plan Legal (R-L).....	289
2.7	Overall Roadmap .....	289
<b>3</b>	<b>ARTICLE 29 WORKING PARTY COMPARISON .....</b>	<b>292</b>
<b>4</b>	<b>LEGAL MATERIAL .....</b>	<b>293</b>
4.1	Electronic Signature .....	293
4.1.1	Types of the Electronic Signature in Comprehensive Law (Europe).....	293
4.1.2	Legal Effects .....	294
4.1.3	Probative Value.....	295
4.2	Pseudonymity .....	297
4.2.1	Legal .....	297
4.2.2	Electronic / Digital Signature.....	297
4.3	Other Legal Material .....	298

---

## List of figures

Figure 1: Overview over Chapter 1 .....	viii
Figure 2: Chapters influencing Chapter 2 .....	ix
Figure 3: Chapters influencing Chapter 4 .....	ix
Figure 4: Chapters influencing Chapter 5 .....	x
Figure 5: Chapters influencing Chapters 6 and 7 .....	x
Figure 6: The "I" and the "Me" .....	2
Figure 7: Structuring the "Me" of the Identity .....	6
Figure 8: Actors within an IMS – an Abstract Model .....	34
Figure 9: Actors within an IMS – an Abstract Model of an Organisation.....	34
Figure 10: An IMS Model in More Detail .....	35
Figure 11: Identity Thief Using Services without Authentication.....	42
Figure 12: Attack Points of an Identity Thief in a Scenario with Authentication .....	42
Figure 13: Data Trails When Using Internet Services.....	43
Figure 14: Typical Logs at Different Parties.....	44
Figure 15: IMA as a Gateway to the World .....	45
Figure 16: Identity Protector and Different Pseudo Identity Domains.....	47
Figure 17: The Identity Protector in an Information System.....	47
Figure 18: Pseudonym Domains in Assignment of Tasks.....	48
Figure 19: Pseudonym Domains of a Customer in an E-Shopping Scenario .....	51
Figure 20: E-Shopping Scenario and Paying with a Credit Card .....	51
Figure 21: Pseudonym Domains of Customer and Seller in an E-Auction Scenario .....	53
Figure 22: The Customer in the (E-)Banking Network .....	56
Figure 23: Pseudonym Domains of a Citizen in an E-Tax Scenario .....	57
Figure 24: Pseudonym Domains of a Citizen in an Inquiry Scenario .....	59
Figure 25: Pseudonym Domains of Plaintiff and Defendant in a Civil Action .....	61
Figure 26: Pseudonym Domains of Accused and Witness in Criminal Proceedings .....	63
Figure 27: Pseudonym Domains of a Voter in an E-Voting Scenario .....	65
Figure 28: Pseudonym Domains of a Patient in an E-Health Scenario .....	67
Figure 29: Pseudonym Domains of Author and Reviewers in a Review Scenario .....	69
Figure 30: Integration of Notaries as E-Witnesses .....	71
Figure 31: The TAM Theory .....	76
Figure 32: Pseudonymity as the Full Range between Identity and Anonymity .....	85
Figure 33: Pseudonyms With Different Degrees of Cross-Contextual Linkability .....	86
Figure 34: Data Flow Concerning Credentials in an IMS .....	88
Figure 35: Form Manager with Choice .....	114
Figure 36: Password Manager and Possibility of Selecting a User .....	116
Figure 37: Form Manager – Possibility to Fill in Automatically .....	117
Figure 38: Encryption When Storing Sensitive Data Activated.....	120
Figure 39: Overview Evaluation Mozilla Navigator .....	124
Figure 40: Passport.....	125
Figure 41: Passport – Profile .....	129
Figure 42: Passport – Registration .....	130
Figure 43: Passport – Malfunction if not using Internet Explorer .....	131
Figure 44: Passport – "Sign me in" .....	132
Figure 45: Overview Evaluation Passport .....	136
Figure 46: Federated network identity and circles of trust by Liberty Alliance .....	137
Figure 47: Liberty Alliance .....	143
Figure 48: Overview Evaluation Liberty Alliance .....	149
Figure 49: Digitalme .....	150
Figure 50: Digitalme – User Can Choose a Situation for the meCard .....	151
Figure 51: Digitalme – Visit to a Foreign meCard after Retraction of Permission .....	152
Figure 52: Digitalme – Register .....	153
Figure 53: Digitalme – VeriSign .....	155
Figure 54: Digitalme – "Who are you?" .....	157
Figure 55: Overview Evaluation Digitalme .....	159
Figure 56: Yodlee – Welcome .....	160
Figure 57: Yodlee – Accounts.....	162
Figure 58: Yodlee – Sign In .....	165
Figure 59: Overview Evaluation Yodlee .....	167
Figure 60: Outlook Express – Switch of Identities .....	168

---

Figure 61: Outlook Express – Management of Identities.....	169
Figure 62: Outlook Express – "Which Identity?".....	170
Figure 63: Outlook Express – "Add New Identity".....	171
Figure 64: Outlook Express – "New Identity".....	173
Figure 65: Overview Evaluation Outlook Express.....	176
Figure 66: CookieCooker – Main Window .....	177
Figure 67: CookieCooker – Web Interface .....	177
Figure 68: CookieCooker – Web Interface: "Identities..." .....	178
Figure 69: CookieCooker – Cookies and Identities .....	179
Figure 70: CookieCooker – Configuration.....	180
Figure 71: CookieCooker – "Select Identity!" .....	181
Figure 72: CookieCooker – Malfunction Understanding .....	182
Figure 73: CookieCooker – "Delete old Cookies" .....	184
Figure 74: CookieCooker – JAP Integration .....	186
Figure 75: Overview Evaluation of CookieCooker.....	187
Figure 76: ATUS – Components.....	188
Figure 77: ATUS – Architecture .....	189
Figure 78: ATUS – Snapshot PDA Version.....	189
Figure 79: DRIM – Architecture and Available Components.....	190
Figure 80: DRIM – Internal Structure of the Client .....	191
Figure 81: DRIM – Creation of Pseudonyms.....	192
Figure 82: Basic Model: IMA ↔ Application ↔ Digital Services.....	201
Figure 83: Basic Model: Application ↔ IMA ↔ Digital Services.....	201
Figure 84: Basic Model: IMA in Application ↔ Digital Services.....	201
Figure 85: Limited Trusted Zone .....	202
Figure 86: Enhanced Trusted Zone .....	202
Figure 87: Architecture of a Privacy-Enhancing IMA .....	205
Figure 88: Comparison EU vs. Non-EU Activities on IMS (from Chapter 3).....	207
Figure 89: PIM in RAPID's Vision .....	215
Figure 90: Roadmap: Market Penetration Techniques.....	216
Figure 91: Roadmap: Market Penetration of IMS .....	218
Figure 92: Roadmap: Maturity of Concepts and Applications for IMS .....	221
Figure 93: Institutional Background of Responding Experts .....	227
Figure 94: Positions of Responding Experts in Their Organisation.....	228
Figure 95: Cultural Background of Responding Experts .....	229
Figure 96: Interests of Responding Experts .....	230
Figure 97: Marketability of IMS .....	235
Figure 98: Important Aspects of an IMS .....	237
Figure 99: Effects of IMS on Law Enforcement Respectively Prosecution of Claim.....	240

---

## List of tables

Table 1: Requirements in the General IMS Scenario .....	46
Table 2: Requirements of the Processing of Orders Scenario .....	49
Table 3: Requirements of the E-Shopping Scenario .....	52
Table 4: Requirements of the E-Auction Scenario .....	54
Table 5: Requirements of the E-Banking Scenario .....	56
Table 6: Requirements of the E-Tax Scenario .....	58
Table 7: Properties with Respect to Extract from the Register .....	59
Table 8: Properties with Respect to Freedom of Information .....	59
Table 9: Properties with Respect to Access according to Data Protection Acts.....	59
Table 10: Requirements of the Inquiry Scenario.....	60
Table 11: Requirements of the Civil Action Scenario.....	62
Table 12: Requirements of the Criminal Proceedings Scenario.....	64
Table 13: Requirements of the E-Voting Scenario.....	65
Table 14: Requirements of the E-Health Scenario .....	68
Table 15: Requirements of the Review Scenario .....	69
Table 16: Requirements of the E-Witness Scenario .....	72
Table 17: Summarisation of Requirements of Scenarios .....	73
Table 18: IMS Mechanisms with Respect to Requirements.....	82
Table 19: Technology-based IMS Mechanisms with Respect to Co-operating Parties.....	93
Table 20: Basic Criteria .....	95
Table 21: Criteria Operational Areas .....	96
Table 22: Miscellaneous Criteria .....	96
Table 23: List of Identity Management Applications Ordered by Availability and Nations.....	98
Table 24: List of Existing Identity Management Applications .....	101
Table 25: Description of Functionality .....	105
Table 26: Description of Categories.....	105
Table 27: Description of Platform and Environment .....	106
Table 28: Compared Identity Management Applications and General Functionalities.....	112
Table 29: Further interesting Approaches of Identity Management Applications .....	112
Table 30: Comparison of Identity Management Applications .....	198
Table 31: Prediction PC Mass Storage.....	220
Table 32: Prediction Computer .....	220
Table 33: Potential Main Bottleneck Regarding Mass Adaption of IMS.....	235
Table 34: V1 – How Many Years Dealing with IMS.....	262
Table 35: V2 – Employees in Organisation ... .....	262
Table 36: V3 – Organisation and IMS ... .....	263
Table 37: V4 – Other Organisation .....	263
Table 38: V5 – Position in Organisation .....	263
Table 39: V6 – Other Position .....	264
Table 40: V7 – Do You Already Use an IMS? .....	264
Table 41: V8 – For Which Application? .....	264
Table 42: V9 – With Which Product? .....	265
Table 43: V10 – Interests in IMS ... Range of Functions .....	265
Table 44: V11 – Interests in IMS ... Usability.....	265
Table 45: V12 – Interests in IMS ... Privacy Protection.....	266
Table 46: V13 – Interests in IMS ... Security.....	266
Table 47: V14 – Interests in IMS ... Marketability.....	266
Table 48: V15 – Interests in IMS ... Politically Pushing Through .....	266
Table 49: V16 – Interests in IMS ... Politically Preventing it .....	266
Table 50: V17 – Interests in IMS ... Implementing Law .....	267
Table 51: V18 – Interests in IMS ... Social Impacts of Implementation / Use .....	267
Table 52: V19 – Interests in IMS ... Potential Psychological Consequences .....	267
Table 53: V20 – Interests in IMS ... Law Enforcement.....	267
Table 54: V21 – Interests in IMS ... Access Right Management .....	267
Table 55: V22 – Interests in IMS ... Multiple Application Usage .....	268
Table 56: V23 – Interests in IMS ... Another Important Category .....	268
Table 57: V24 – Interests in IMS ... Another Important Category .....	268
Table 58: V25 – Cultural Background .....	268
Table 59: V26 – IMS – State-of-the-Art .....	269
Table 60: V27 – IMS – Essential Functions .....	269

---

Table 61: V28 – IMS – Marketability .....	271
Table 62: V29 – IMS – Marketability in 10 Years.....	271
Table 63: V30 – How Long Will it Take for a Society-Wide Implementation of a Multi-Purpose IMS?271	271
Table 64: V31 – IMS – Important for Use in Society – Range of Functions .....	271
Table 65: V32 – IMS – Important for Use in Society – Multi-Purpose Usage .....	272
Table 66: V33 – IMS – Important for Use in Society – Usability.....	272
Table 67: V34 – IMS – Important for Use in Society – Privacy Protection.....	272
Table 68: V35 – IMS – Important for Use in Society – Security .....	272
Table 69: V36 – IMS – Important for Use in Society – Cost .....	272
Table 70: V37 – IMS – Important for Use in Society – Controllability for Users .....	273
Table 71: V38 – IMS – Important for Use in Society – Controllability for Government .....	273
Table 72: V39 – IMS – Important for Use in Society – Tracing of Law Enforcement.....	273
Table 73: V40 – IMS – Important for Use in Society – Other Category.....	273
Table 74: V41 – IMS – Important for Use in Society – Specified Category.....	273
Table 75: V42 – Administration of Data.....	274
Table 76: V43 – Administration of Data – Some Comments.....	274
Table 77: V44 – Psychological Consequences.....	274
Table 78: V45 – Specified Psychological Consequences.....	275
Table 79: V46 – IMS – Improve or Worsen – Liability .....	276
Table 80: V47 – IMS Improve or Worsen – Crime Prosecution.....	276
Table 81: V48 – IMS Improve or Worsen – Clarification of Facts.....	276
Table 82: V49 – IMS Improve or Worsen – Value of Admissible Evidence .....	276
Table 83: V50 – IMS Improve or Worsen – Other .....	277
Table 84: V51 – IMS Improve or Worsen – Specified Other .....	277
Table 85: V52 – IMS – Bottleneck .....	277
Table 86: V53 – IMS – Bottleneck, Other .....	278
Table 87: V54 – Visionary IMS Texts .....	278
Table 88: V55 – Published IMS Texts .....	279
Table 89: V56 – Commentary .....	281
Table 90: V57 – Answers.....	282
Table 91: V58 – Syntax.....	282
Table 92: V59 – Reminder .....	282
Table 93: Return Quota .....	282
Table 94: Research Cluster PET in Enterprise .....	285
Table 95: Research Cluster PET in Infrastructure.....	287
Table 96: Research Cluster Multiple and Dependable Identity Management .....	287
Table 97: Research Cluster Socio-Economic PIM .....	288
Table 98: Research Cluster Legal Aspects PIM .....	289
Table 99: Selection of the Essential and Important Technology Business RTD for PIM .....	290
Table 100: RAPID Roadmap .....	291
Table 101: Comparison of the Presently Existing On-line Authentication Systems .....	292



# 1 [CHAPTER A: DEFINITION OF IDENTITY MANAGEMENT SYSTEMS]

This Chapter deals with the sociological, legal and technical aspects of identity and identity management, and the central terms for this study will be defined. Sociologically, the constitution of personal identity by specific communication in specific different social contexts will be addressed. Legally, mainly the present legal position in Europe will be pointed out with a view on the surprisingly flexible identity construction. A view onto history will show the plausibility of this increasing flexibility. Regarding the technical implementation of identity management, the technology-based management of pseudonyms will be the main subject of discussion.

This study focuses on the user-controlled management of own identities rather than describing systems which only do user profiling without offering the individual a possibility to manage that data in databases or data warehouses. This second type of self-called "Identity Management Systems" is found quite often in today's business, but in contrast to the user-controlled Identity Management Systems they concentrate on business processes rather than comprising the user's point of view. With our notion of IMS, putting the user in the centre, but nevertheless discussing possible implications also for organisations of different kinds, we take into account, that IMS in fact create a new paradigm in the sociological, legal and technological worlds.

We distinguish between the whole Identity Management System (IMS) with its infrastructure and the Identity Management Application (IMA) which can be installed, configured and operated at the user's and/or a server's side. Finally, typical actors and their tasks in an IMS-supported setting are identified. For introduction we define technology-based identity management as follows:

Technology-based identity management in its broadest sense refers to administration and design of identity attributes.

## 1.1 Definition of Identity

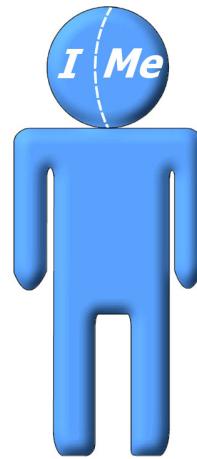
### 1.1.1 Identity from the Sociological Perspective

#### 1.1.1.1 Identity

Definitions around the concept of "human identity" usually define the term "identity" from the difference between the public and the private aspects of a human.

Thereby, identity is explained as an exclusive perception of life, integration into a social group and continuity, which is bound to a body and shaped by society. Such concepts of identity modify the difference between "I" and "Me" [cf. Mead 1934].

By this definition, "I" is the instance that is accessible only by the individual self, perceived as an instance of liberty and initiative. "Me" is supposed to stand for the social attributes, defining a human identity that is accessible by communications and that is an inner instance of control and consistency. Identity describes the distinction between an individual and a person, which can only be determined from the perspective of the person. The role then denominates the interrelation between activation of situation dependent identity properties and the corresponding form of the transmitting action.



**Figure 6: The "I" and the "Me"**

Besides the epistemological evidence for the social constitution of the concept of "identity" (and "man", "individual", etc.), one can further remark that the relation between "I" and "Me" that is constitutive for identity has been described as an "introverted social relation", one between "I" and "Me". From a constructivist-sociological standpoint, we recognise "identity" within our own respective stream of consciousness, or what we try to describe with scientifically controlled methods, is really constituted communicatively and socially. Hitherto, the socially constituted concept of "identity" creates the observability of human attributes and qualities commonly called unique.

A recent compact socio-psychological definition describes identity as the "... permanent inner being one with oneself, the continuity of experience of one-self (self-identity) which is, for the most part, created by assuming certain social roles and membership in groups, as well as by recognition by someone who has assumed these roles or belongs to the respective group" [Fuchs et al. 1978].

The exclusive self-observation of a human will find its limit where the "I" aspect of identity becomes incomunicable and no terms for its denomination are available. This is the point for which one could probably claim a maximum or maybe the complete absence of individual uniqueness, unmistakability and spontaneity. Only, it is impossible to describe it in words. The determination of identity names the interface of a pre-lingual instance of the individual with a person's social – i.e., communicatively accessible and addressable – social integration. The decision about a point in time for activation of a personal attribute, the combination of attributes in past and present and the respective profile of attributes are individually unique. Together with the social constraint of identity profiles the individual aspect of a human's identity, which integrates all of these aspects, becomes visible for the first time. Identity is communicable, as long as it is possible to name it. Therefore, this form of identity is also technically-operational accessible.<sup>7</sup>

If the "identity" of an individual in the form of a person can be described as mostly socially formed, it becomes necessary for the developing of the complexity of identities to distinguish the social contexts in which persons navigate and in which some of their *partial identities*<sup>8</sup>,

<sup>7</sup> Jumping ahead a bit, we would like to remark that the established terminology of "identity management" is a somewhat arbitrary one. On the one hand it is a functional notion insofar as it has found increasing resonance in organisations of social subsystems of economy, law, politics and science. But it will possibly active unnecessarily the complex, deep reaching psychological and philosophical context that will usually be associated with the term "Identity", at least in the use of the word in German language. It would probably be more appropriate and would require less demanding conceptual work of narrowing down the subject of work, if one would more modestly talk about "addressing management" and the resulting problems and issues. On the other hand, the term "addressing management" could be too narrow in the same sense that "identity management" is possibly too broad. The advantage of the use of the term "identity management", at any rate, is that it has by merit of its heavy meaningfulness a certain alarming function. At least intuitively, it is evident that new arrangements between persons and organisations can be expected in the future.

<sup>8</sup> In the sequel, we might leave out "partial" and using the shorter "identities" if the meaning is clear from the context.

bundles of attributes of their complete identity, become relevant. On a technical level, these attributes are data.

### 1.1.1.2 Typology of Social Systems

The factual area of modern social sciences, more to the point, of social system theory, is constituted by social systems. A social system is viewed as a special entity of its own kind, reproducing itself from system specific communication.

From a standpoint of sociology, three types of social systems can be distinguished:

- a) Interactional systems
- b) Organisational systems
- c) Social subsystems

a) Interactional systems are being generated and reproduce among present persons when these recognise that they recognise each other and participate in communication. For instance, one would think of spontaneous encounters, such as in a shopping mall, in a train compartment, flirting and the careless talk among friends. A specific, sociological viewpoint is being introduced when it is noted that communication begins at all and that no arbitrary but thematically tapered communication and actions are effected. May the participants view their specific contributions to such communication as extremely individual, an external observer will not usually find it difficult to categorise such interaction because of its general dissemination.

b) Among organisational systems, such diverse entities such as administration, enterprises, clubs, institutions, institutes, political parties, hospitals, schools, monasteries, prisons, armies can be counted. These reproduce according to decisions that are being recycled out of previous decisions in which the members participated, who are subject to defined for joining and separation. Organisations differ from one another, e.g., in decisions regarding the empowerment of their members. In prisons, a very strict, hierarchical structure exists, where prisoners may have a consultative, but never a decision right for changing of structures. In smaller start-up companies, the structure is usually a lot more complex, at least as along as the motivation of the employees with regards to achieving the organisational goals is not in doubt. A material discussion of the functioning of organisations must be based on the distinction between (internal) members and (external) clients.

c) Social subsystems reproduce by means of communication that is being introduced through symbolically generalised communication media. Up to now, four types of social systems have been identified with certainty: The economical system, which reproduces itself according to the differentiating codes of payment/non-payment (program: price), the legal system, which reproduces itself based on the codes of legal/non-legal (program: laws), the political system, which reproduces itself based on the codes of power/non-power (program: programmes), and the scientific system, whose communication is formed based on the difference between true and false (program: theories and methods). Therefore, the economic system is a communicative context reproducing itself along payments. Sociologically, it is not viewed – we have to mention this because it is a common picture – as an emergent aggregation of organisations or of rational economical actors whose primary goal is an optimal return on capital investment.

These rather coarse elaboration on system typology of social system theory and reference to in-depth literature have to suffice for this study.<sup>9</sup> These remarks should however be sufficient to give an impression of where the differences between the constitution of identity within different social contexts are, that are being made manageable by "identity management".

---

<sup>9</sup> Introduction to Social System Theory: Luhmann 1987; Kiss 1990, Kneer/Nassehi 1993; Interaction Systems: Kieserling 1997; Organisational Systems: Baecker 1999, Luhmann 2000; Social Systems: Luhmann 1997.

---

### **1.1.1.3 Identity in Interaction Systems**

In Interaction systems, the identity of a person has a special relevance. One views each other, hears the voice, sees the posture and thereby deduces the emotional state of a person. The identity of a person is not problematic here, as identity is simply being viewed as an unchangeable attribute of a person. One knows the specific character of the other; his attributes can be viewed as an analytically undivided whole. Comparatively, individual and person do not come very far apart.

Should it not be possible to establish congruence of identity ("I am who I am.") and authenticity ("I am who I claim I am.") in the course of identification ("Who are you?" – "But I am your old friend"...) or authentication ("Are you who you say you are?" – "You must recognise me! I am your old friend!"), this will be cause for conflicts in interaction system. Truthfulness and stability in appearance are demanded and expected. Names play a less important role for identification in interaction systems. They are being said in order to address a message within a group as directly as possible or in order to emphasise the importance of a message. It is sufficient to exclaim a first name or a nickname, followed by looking at the person. One is moving in listening distance. The formal requirement for identification is low, the requirement for identification as such, on the other hand, is very high. One wants to know exactly who the other party is. At the moment of first encounter, a visual impression is taken and based on a multitude of biometric properties, the identity of the other person is established.

The requirement for formal collections of personal data exists only from that point in time onwards, when besides interaction systems – with regards to social evolution also called segmentary societies – also organisational systems have been established, which at least temporarily require a more context dependent interaction. Mutual assessment of physical properties is no longer sufficient in order to find the correct mode of interaction.

### **1.1.1.4 Identity in Organisational Systems**

The constitution process of identity is far more complex in organisational systems, because in organisations the distinction between identity and authenticity has far greater relevance. One person in an organisation is not only what the person thinks she is, but also what the organisation thinks. A person isn't only the one she claims to be, but also always another one. Other than in interaction, this difference doesn't result in conflict within an organisation. On the contrary: Those persons who are unable to manage their partially logically irreconcilable roles pragmatically as different roles, will have a more difficult time in organisations. Only because of the issues resulting out of this differentiation, something as the concept of identity, the separation of a public persona and a private individual, has historically evolved.

This separation can be highlighted in history in the instance of family names and evolution of the first kind of information technology in the form of writing. In the beginning, inheritable family names were loosely connected to a person. With the evolution of urban societies more stable family names evolved, which were describing either towards the origin (counties ("westfal")) or lodgings ("doorman")), the profession (trade ("merchant"), craftsmanship ("Wagner") or agriculture ("Huber")).

"The inherent tendency towards consolidation was promoted through registration of family names in lists of citizens, tax lists and registers of interest, which became necessary as a consequence of the grown number of inhabitants and an increased rate of legal interaction. The written registration can be seen metaphorically as the moment of birth for family names, although until into the 16th century a certain flexibility was still recognisable and some rare or unpopular names disappeared again" [cf. Bahlow 1985: 8]

With the introduction of written documentation promoted by the inception of organisation and the slowly evolving functional differentiation of social systems, the necessity for switching between the person and the individual increasingly often arises.

A person is always more and other things than that what is currently being actualised in communication. An organisation explicates the functions relevant for itself and thereby generates a requirement for persons and attributes. "Addresses" with regards to persons with names or relating denominations are the crucial point for communication with and within organisations. Generally, stable addressing relations are a central factor for the authenticity of action for organisations, internally as well as externally.

In the course of increased importance of organisations, the former meaningfulness of family names diminished. In modern societies, and with only very few exceptions, they only serve as abstract, context-less identifiers. Different organisations with different functional objectives only ever use a certain subset of addresses from the total of possible personal attributes or constitute a context relevant personal identity. Because the function of organisations today is in an addressable synthesis of the functions of the social subsystems economy, law, politics and science, the demand for formal data only geared to these systems and addressable attributes. It is recommendable to use the term "addressable attributes" because besides persons, also computing systems and organisations have to be considered as addressable, and because consequently one has to consider the identity of computing systems and organisations! Not taking into account for a moment this somewhat daring hypothesis, it is noted that organisations need to co-ordinate structures of social subsystems with corresponding personal attributes. Therefore, today a person's name, gender, date of birth, size, eye and skin colour and social properties count among personal data, along with functionally relevant aspects such as number of children, religious confession, education, profession, creditworthiness, nationality, aspects confirming legal capacity or special attributes for scientific inquiries.

#### **1.1.1.5 Identity in Social Subsystems**

Like interaction systems and in contrast to persons and organisations, social subsystems are not addressable. They operate in communicatively interdependent contexts. Therefore, no identity related attribute (and, we remark, no capability of action) could be communicatively assigned to them. Still, they play an important part in constituting personal identity. For instance, a person who is seen as insolvent due to unemployment, who is incapacitated due to mental illness or perceived to be insane or who because of his origin or nationality is lacking the right to vote or to participate in political discourse, is impaired in her or his identity. She or he can only participate in socially relevant communication in a limited way, with a resulting depressing effect on the individual self-perception. Systemically, this is described as a functional identity.

The addresses these systems have communicative access to, do not need to be material or with regards to concrete individuals be matched by biometric attributes. Here, we generally speak about "the customer" in his broadest sense, "the citizen", "the autonomous individual", "the patient", "the test person", "the homo oeconomicus" or other scientifically tapered variations of a person. In so far, these systems generate the impression that much of this functionally tapered communication in the form of, e.g., payments, elections, legal motions, valuations of scientific publications can or, more pointedly, needs to take place anonymously in order not to regress to an only organisational level.

These functionally tapered social systems provide organisations and persons with a socially relevant supply of topics. Based on prices, laws, programs, theories and methods even improbable calculus can be developed and decisions being taken. The topical relation to a functional system, the mechanisms of the trust-based securing of a relationship between organisation and client and the personal data used hereto determine the socially and functionally necessary extent of data and processes.

#### **1.1.1.6 Technologically Supported Identity: Digital Identity**

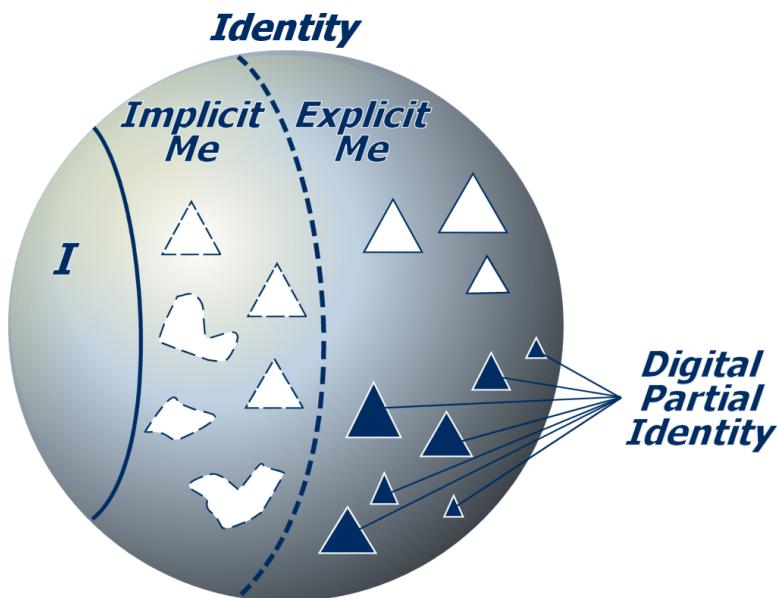
The term *Digital Identity* usually denotes two distinct topical areas. On the one hand, the term has gained popularity with all authors speculating about the expected psychosocial impact of the

use especially of the Internet [cf. Turkle 1995, Döring 1999]. Until the mid 1990s, there was a lot of discussion about a "multiple personality" [cf. Lehnhardt 1995]. The assumption that new experiences in handling new forms of communication will lead to new concepts of identity has become a lasting part of sociological theories about the Internet [cf. Hoffmann 1997]. The analysis of so-called Multi-User Dungeons (MUDs) [cf. Berman/Bruckman 2001] or of artificial actors in avatar worlds and their "playing with identities" [Schetsche 2001] has left a lasting impression.

In this study, we will not use the term *Virtual Identity*, playing an important role in the context of technically supported identity. The attribute "virtual" puts identity into a thematic context with "unreal, non-existent, seeming" and that may apply to characters in a MUD or to avatars. With the increasing self-evidence and every-day use of Internet usage, the subconsciously associated, culture-pessimist-critical impetus denoting a virtual or digital identity as defective compared to a "real world" identity, apparently slowly dissolves.

Digital identity can also denote the much more factual aspect of attribution of properties to a person, which are technically immediately operatively accessible. More to the point, a digital partial identity<sup>10</sup> can be a simple e-mail address in a news group or a mailing list. Its owner will attain a certain reputation. More generally if we consider the whole identity as a combination from "I" and "Me" where the "Me" can be divided into an implicit and an explicit part (cf. Figure 7):

Digital identity is the digital part from the explicated "Me".<sup>11</sup> Digital identity should denote all those personally related data that can be stored and automatically interlinked by a computer-based application.



**Figure 7: Structuring the "Me" of the Identity**

In this way, this study uses the term identity in the context of technically supported identity management [cf. Clarke 1993<sup>12</sup>/1999; Jendricke/Gerd tom Markotten 2001].

<sup>10</sup> A *digital partial identity* is the same as a *partial digital identity*. In the sequel, we skip "partial" if the meaning is clear from the context.

<sup>11</sup> Note that there is also a non-digital part of the explicated "Me", but the trend of digitisation leads to a shifting towards the digital part.

<sup>12</sup> "Digital identity is the means whereby data is associated with a digital persona. Organisations which pursue relationships with individuals can generally establish an identifier for use on its master file and on transactions with or relating to the individual. [...] There are three approaches whereby a digital identity can be constructed from multiple sources: a common identifier; multiple identifiers, correlated; and multi-attributive matching."

The mechanisation of (the (self-)management of) person-related identity attributes has several important consequences which we want to describe shortly, because they have a relevance for the design of an Identity Management Application ("IMA"), especially as seen from the perspective of the user. The attributes of personal identity are explicated through their technical implementation. What was not segregated up to now, neither attributed to "Me" nor "I", will be segregated through explication.

Regarding the future impact of IMS it can be expected that the process of explication will not halt until the appearance of a certain practical completeness has been generated. The more details a personal knows about its owners Digital Identity, and the more precisely it knows them, the more satisfyingly it will fulfil its mission [cf. Nabeth/Roda 2002]. Corresponding to this development of increasing the resolution of Digital Identity, only that, which is implicit and therefore incommunicable, remains with the "I". Hence, metaphorically turning out to be the individual side of identity, the "I" increasingly turns out as an irrational instance that is less and less communicatively reachable. With the explication of an identity's attributes comes the explication of communication. The communication history with other persons gives rise to an explication of a person's social network. Relationships hitherto ambiguous to mutual advantage, e.g., oscillating between friendship and a commercial or employer-employee relationship, will be increasingly explicated. The mixture of formal and informal relationships, which plays an important role in interactions between organisations and private persons, loses its informal side, which has so far been an efficient means for regulation of conflicts.

Explication corresponds to a standardisation of denominations of identity attributes, facilitating the automated processing of these attributes. Automation of information processing can be seen in the tradition or as the consequential continuation of the industrialisation project [cf. Hansen/Rost 2002]. Especially computer networks give rise to the genesis of "data shadows", which are beyond the control of those throwing these "shadows". In reaction to this development, which has become visible very early, the German Federal Constitutional Court postulated a "right to informational self-determination" in 1983.<sup>13</sup> Its technical implementation and further development is the goal of "Privacy-Enhancing Technologies".<sup>14</sup>

Hereafter, we want to develop the requirements for management and administration of identity according to the differentiation of communications and social systems, because we see that the user's expectations towards identity management are largely being determined by the communicative requirements. Of course, the requirement for a design of man-machine-interaction in accordance with recognised medical-anthropological-cognitive conditions of human information processing stays intact. This aspect will be treated under the headline of "Usability".

### 1.1.2 Identity from the Legal Perspective

Today's most broadly accepted definition of legal person is a human being to which the legal systems refers rights, privileges and obligations [cf. Kelsen 1966]. The legal systems of democratic and advanced societies also consider human organisations (companies, partnerships, family, foundations, associations and other private or public entities) as point of reference of rights and obligations. The most traditional reconstruction of the "legal person" has been theorised at the end of the 19<sup>th</sup> century as a "*fictio juris*": a legal entity is a subject of rights and obligations, thus an *individual*, as far as the law provides accordingly [cf. Savigny 1888]. Anyway it is possible to affirm that in juridical sciences the concept of legal personality is, like in psychological and sociological sciences an *a posteriori* that resumes all the aspects (functions, qualities, effects) that are linked to a same (id-)entity [cf. Bianchi 1963].

<sup>13</sup> "The individual [...] has the right to know and to decide on the information being processed about him." ("... Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.") – German Constitutional Court in BVerfGE 65, 1, 41, 1983.

<sup>14</sup> The term comes from John Borking who used it first in the context of the "Identity Protector" [van Rossum/Gardeniers/Borking et al. 1995].

---

Ancient legal systems often referred rights and obligations not to a single person, but to a family or a tribe ("*Gens*" in ancient roman law (cf. Ruiz 2002; Manfredini 2001) and "*Stamm*" in ancient German law). Anyway already at the end of the first millennium most legal systems referred rights and obligations to individuals (and not to tribes), with the exception of slaves, of the *adscripti*, or of the *colones*, that where mostly objects of rights and obligations [cf. Winfield 1925].

Most part of history, identity has been understood by legislation only as a tool to assess/verify the subject to which refer rights and obligations (and punishment for trespassing law). Only with the constitutional acknowledgement of individual liberties with the first constitutions during the Enlightenment, identity became also expression of individual freedom and of liberty [cf. APPENDIX: "Amendments to the US Constitution"]. It has to be considered that at the end of the 18<sup>th</sup> century in France even if there was the general right to vote, this was in fact granted only to male citizens, paying 6 *livres* or more of *capitation*, older than 25 years, registered at the fiscal authority, if living autonomously [cf. Rude 1911]. The way to a full recognition of all individual rights was still far from being accomplished. This has not to surprise. Psychology as science (and thus the concept of personality as a scientific category) was still not accepted by scholar science in the 19<sup>th</sup> century<sup>15</sup>. How could legislation regulate systematically something of which there was no scientifically or socially accepted definition? Therefore the approach was a case by case approach, taking into consideration mostly:

- a) Identification techniques, in particular in the first half of the 20<sup>th</sup> century and
- b) Protection of one's reputation and honour (in particular the limits of self enforcement of violations of the honour of an individual).

In fact only starting from the beginning of the 19<sup>th</sup> century, identity as one aspect of personality has increasingly become recognised by law also in order to ensure proper expression of individual personality and of freedom of people to establish (non armed) organisations.

Under current legislation, the identity of physical persons in legislation has no systematic regulation. It is a stratification of definitions, which do not always match with each other and has two main functions:

- a) To grant identification for legal purposes and
- b) To protect individual rights of freedom (name, identity, self determination, freedom of speech, privacy, etc.) related to a physical person.

Hence identity is made by elements with the function to grant its uniqueness and by (other) elements that are the expression of human identity with all its possible (and individually, freely chosen) aspects.

The technological evolution has allowed since the first half of the 20<sup>th</sup> century to begin with biometric identification, through the use of photography on the personal documents.

The elements with the function of grant uniqueness to a personal identity are in most developed legal systems:

- a) Gender (male/female);<sup>16</sup>
- c) Name (given name);<sup>17</sup>
- d) Surname (family name);<sup>18</sup>

---

<sup>15</sup> Even if psychology as such was first theorised by Rudolf Göckel (Glorenius) in 1590, it was still treated as a philosophical theory of/on the human spirit (totally complying with the ancient Greek philosophical tradition, culminating in Aristotle's fundamental work "*De Anima*").

<sup>16</sup> Under European law it is not possible to give a male name to a person of the female sex and vice versa.

<sup>17</sup> The name is an identifying element in all European countries, and most international country.

- 
- e) Date of birth;<sup>19</sup>
  - f) Place of birth;<sup>20</sup>
  - g) Number of the birth certificate;<sup>21</sup>
  - h) Identity of the parents;<sup>22</sup>
  - i) Nationality;<sup>23</sup>
  - j) Place of residence/domicile;<sup>24</sup>
  - k) Profession.<sup>25</sup>

They will be treated in Chapter 1.1.2.1.

The aspects of the human personality granted by the (constitutional) legislation of democratic legal systems, regulated by private law and also protected against unilateral unauthorised aggression by third parties are:

- 1) The name and the identity;
- 2) Freedom from physical constriction (habeas corpus);
- 3) Inviolability of the domicile and right of privacy;
- 4) Freedom of speech and self expression, in particular two sub-categories of it:
  - The right to choose one's image;
  - The right to protect one's honour;
- 5) Freedom of movement and to settle (granted only to fully aged people).

They will be treated in Chapter 1.1.2.2.

### **1.1.2.1            The Elements of Identity that Ensure its Uniqueness**

The personal identity is regulated at constitutional level, by the treaty of the European Union, by national private legislation, and protected by rules of the criminal law, against unduly unauthorised interference by third parties.

Moreover administrative law regulates personal identity.

For the fundamental scopes explained in the next Chapter, it is defined as the complex of the personal data results contained in the public registers, reported on identification documents, which serve to identify the persons towards individuals and public administration and to distinguish the said person from the consociates.

---

<sup>18</sup> The surname is an identifying element in all European countries and most international countries. In some states (India, Pakistan, Nepal, Somalia; Ethiopia) there is no difference between given name and family name. In the Egyptian passport are indicated more names: the first is the given name, the second is the father's name, the third is the grandfather name and the fourth is the surname. In Filipino and Bulgarian passport is indicated also the patronymic.

<sup>19</sup> In the most countries it is an element of identity, but there are some exceptions (for example Spain). In Morocco it indicates only the year of birth.

<sup>20</sup> Austrian and Spanish legislation does not consider the place of birth to be an identifying element. In the USA as place of birth are indicated the country and the federal state, In Japan in no document is indicate the place of birth.

<sup>21</sup> In Greece and Slovakia the birth certificate number is a necessary element. In Spain there is instead the National Identity Number. In Italy the number of birth certificate was part of the identification elements, progressively substituted by the fiscal code.

<sup>22</sup> In Greece and Spain the parents' identities must be indicated, as well in Egypt, Brazil and Bulgaria. In Italy, indication of paternity is no longer required following the provisions made Italian Law 31 no. 1064 dated October 1955, which also contains rules concerning personal details in legal extracts, deeds and documents. Article 2 of this law in fact establishes that the indication of paternity and maternity is omitted from all those deeds, declarations, denouncements or documents, in which the person is shown for purposes other than that concerning exercise of the duties or rights stemming from the status of legitimacy or filiation, whilst Article 3 establishes that, in all cases when this omission is applied, the place and date of birth must be indicated.

<sup>23</sup> In every country. The citizens of Hong Kong which have a British passport BNO don't have a British nationality.

<sup>24</sup> Only in Slovakia, Holland and Germany.

<sup>25</sup> In Italy after the Privacy Directive implementation it not necessary to indicate in the ID card the profession. It still is in all notary acts.

---

The identity elements, which guarantee its uniqueness consist of, according to the Italian law<sup>26</sup>, the identification data, surname<sup>27</sup>, name, date and place of birth, name of the parents, these are the first identifying elements of the person since they are inserted upon the birth, in the birth certificate.

In Switzerland the place of birth is not considered in identification, instead it is the place of origin of the Family. An information that is hardly compatible with the principle of data minimisation.

In Italy since 1955<sup>28</sup> the identification of a person was also carried on through the name and family name of father and mother. This has been abrogated, because discriminating against those that had only one known parent or none<sup>29</sup>.

Before the first directive on data protection was introduced into Italian legislation, also the habitual activity/profession, and the civil status (married, unmarried, divorced, widower) were part of the information that was displayed on identity cards in Italy<sup>30</sup>.

Then more information is available on a person, the more unique he/she is. On the other hand such information, like civil status and profession, are considered by legislation now superfluous for personal identification because already too deeply linked to the private sphere of individuals. The public interest of a more accurate identification had to recede before the protection of individual rights of liberty.

Clearly legislation has moved in most democratic legal systems towards techniques of identification that are less intrusive, even if less reliable, than the traditional ones.

The principle that official identification has not to display any information on the private life of the subject to be identified can be indicated as a generally accepted rule. An identification technique that complies with the practical need to be able to differentiate one individual from all others, has to follow two fundamental rules:

- a) Display enough information to ensure to the highest possible degree of security, that the given individual can be differentiated from any other with whom he will possibly come into contact;
- b) Not to display information that goes too far into the private of the subject to be identified.

Normally in order to achieve this each legal system has a set of information available on their identification documents provided with a biometric image of one or more parts of the body of the subject to be identified.

Anyway, in some countries (Austria and UK for an instance) there is no obligation to carry on any identification document. In other countries (Italy and Germany, for an instance) there is an

---

<sup>26</sup> Italian Presidential Decree no. 396 dated November 3rd 2000.

<sup>27</sup> The surname or family name was fundamental in Roman Law, because it expressed membership of a Gens (Family). Barbarian populations in Europe did not make use of the family name, so that with the barbarian invasions, the use of family names had become less common in Europe between the IV Century and the end of the first Millennium. It is interesting to note that, where there was no use of family name, there was in any case a reference to an ancestor or a place of origin of the *Sippe*. Sippe became *Geschlecht* when membership of a certain bloodline of descendants was reintroduced as part of the personal name. In Europe it was in Venice that widespread use of family names was first documented: the first official documents where a family name was used date back to 819 AD [cf. Spagnesi 1978].

<sup>28</sup> Italian Law no. 1064 dated 31/10/1955 established omission of the indication of paternity and maternity in all deeds and documents not serving the purpose of exercise of duties and rights stemming from the status of legitimacy or filiation, as well as in all identity documents. This law, making reference to Article 30 of the Italian Constitution was specifically intended to protect illegitimate children (i.e. children born out of wedlock).

<sup>29</sup> In this case documented identification specified that the parents were N.N. "Non Noti", unknown. Not much short of a mark of infamy.

<sup>30</sup> Article 2 of Italian Law 127 dated May 15th 1999 and Law no. 191 dated June 16th 1998 made indication of occupation and family status optional.

obligation to carry always an identification document. In the first case (Austria and UK) the individual freedom not to justify one's identity is considered more valuable, than the practicality of law enforcement<sup>31</sup>.

### **Scope of Personal Identification in a Legal System and its Limits**

Current legal systems normally appoint/recognise rights and obligations on single individuals. This was not always the case. One of the reasons to assign rights to families or tribes, was that they were more easily recognisable, than individuals. The recognition was carried out through their place of origin/domicile. The rule of relations that were internal to the family/tribe was out of the reach of law.

When identification techniques became more sophisticated and the state began to have an efficient bureaucracy, the reach of law extended to the individuals that started to enjoy an increasing protection by the rule of law also within the family/tribe.

This innovation required the ability to distinguish between different brothers, maybe twins. To this purpose as long as there were no reliable registrars of birth (earliest in the 15<sup>th</sup> century), the personal identification was carried out using mainly place of birth, descent, activity and place of domicile. Only later on also the date of birth became relevant. In certain agricultural societies, an individual will not commonly know his or her date of birth.

The extension of law also to inheritance and family, needed appropriate identification techniques and the concept of uniqueness of the identity commonly accepted as an important feature of law.

Uniqueness is important in order to connect legal effects (rights/obligations) to the proper subject.

To this purpose:

1. A link to the ancestors was essential, in order to rule inheritance and family ties.
2. A link to the personal status of the subject (profession, marriage, children) was also very common, in order to assess again the rights and obligation for inheritance and family law.
3. A link to a place is/was essential, because the domicile is and was where normally the most part of the assets of a person was located.

Besides generation and marriage, links between a subject and his/her actions is not a common mechanism of identification. In fact it never has been very reliable, without the use of proper technologies. Such technologies now exists, so that identification can also be carried out through an endless series of registrations of relatively irrelevant actions, giving a transparent end full picture of the subject to be identified.

Many centuries later identity became not only relevant to mark the difference between one person and another, but also as expression of individual personality.

As we have seen in Chapter 1.1.1 dedicated to the sociological definition of identity, identity as expression of individual freedom and self determination is a concept which is at the same time:

- a) Dynamic and
- b) Multiple

This other features of identity are in potential conflict with the need of a proper identification of persons, but are also expression of rights that are constitutionally recognised as more relevant

---

<sup>31</sup> In UK there is an ongoing debate on the opportunity to introduce the identity card. Still the most part of public opinion is against the identity card. Anyway acceptance is growing and the opinion polls show that already there is almost 50 % of acceptance.

---

then law enforcement, like individual freedom, freedom of speech, freedom of self determination.

### **1.1.2.2        The Aspects of Identity that are Protected by Law**

According to the civil law, it is considered a wider representation of the person comprising not only the personal aspects, but also the complex of his/her activities and professional, cultural, ideological, religious, social positions, which are not only protected by the legislation (usually the constitutional one) but also governed by the private law and still further guaranteed by the criminal rules which protect the honour, the personal identity, the physical freedom, the expression freedom of the individuals and their social formations. In this last way, the personal identity constitutes a synthesis of the "history" of each person, which allows the consociates to identify him/her as a well definite person, whose past and present life is characterised by specific events.

The main legal sources of the protection of individual identity are

- a) Constitutions,
- b) International Treaties
  - Treaties of the European Union,
  - European Convention for the Protection of Human Rights and Fundamental Freedoms,
  - European Directives,
- c) National Law,
- d) Other national Regulations.

The aspects of human personality that are protected by the above mentioned legal sources are:

- a) One's name and the identity
- b) Freedom from physical constriction (habeas corpus)
- c) Inviolability of the domicile and right of privacy
- d) Freedom of speech and self expression, in particular:
  - The right to choose one's image
  - The right to protect one's honour
- e) Freedom of movement and to settle (granted only to fully aged people)

### **The Aspects of the Human Personality Granted by the Legislation of Democratic Legal Systems**

The right to personal identity can be defined as species of the wider genus consisting of the personality rights.

The aforementioned rights have as an object the essential characteristics of man, both as single and in the social formation where his/her personality comes about<sup>32</sup> and they govern the respect of the person.

The right to personal identity has been included, together with the rights to moral integrity, sexual identity<sup>33</sup>, informational identity and confidentiality<sup>34</sup> in the open "catalogue" of the personality rights, already comprising the traditional rights to physical integrity<sup>35</sup>, the name<sup>36</sup>,

---

<sup>32</sup> Art. 2 Italian Constitution, Art. 34 French Constitution, Art. 1 Constitution of Portugal.

<sup>33</sup> Italian law 164/82, Art. 29 of Turkey Civil Code (amended by Law no. 3444 of 4 May 1988); Österreichisches Standesamt Nr. 9/1993; Transsexuellengesetz of 10. September 1982; Art. 29 through 29d of the Civil Code Law of 24. April 1985 Holland.

<sup>34</sup> Italian law 675/96; Belgium, Law 11 December 1998; Denmark, Act no. 429 31 May 2000; Germany, "Federal Data Protection act" of 18 May 2001; Greek, Law 10. April 1997 n. 2472; England, "The data protection Act" of 16 July 1998.

<sup>35</sup> Art. 5 Italian Civil Code; French Civil Code Art. 16 through 16.9; Chinese Civil Code Art. 119.

<sup>36</sup> Articles 6, 7, and 8 Italian Civil Code; Republic of Albania Civil Code Art. 5; Chinese Civil Code Art. 99; Vietnam Civil Code Art. 28.

pseudonym<sup>37</sup>, the image<sup>38</sup>, the moral copyright<sup>39</sup>. There are further clear superimpositions and contact relations between the personality rights, according to the private law, and the freedoms and the rights guaranteed by the Constitution, while the assimilation to the personality and status rights and the solidarity subsidiary rights (rights to health, work, food, social security and welfare services) is contested, above all on the basis of precedent.

### *The Treaty of the European Union*

The Treaty of the European Union attributes to the citizens of the Member states of the European Union a real right of European citizenship. The Treaty guarantees: the right to look for an employment in a Member state without the need to have a work permit; the right to study and live as pensioner in another Member state; the right to make purchases inside the European Union without any restriction on the quantities that the persons can take in his/her own Country.

The EC Treaty acknowledges to the European citizen four essential freedoms: the freedom of circulation of persons, goods, services and capitals inside the European Community. For example: who moves from a Member state to the other can take a job at the same conditions of the citizens of the hosting country (Art. 48 EC Treaty), can carry on further an independent job, by settling himself/herself in a permanent way (Art. 52 EC Treaty) or for a determined period of time in another country (Art. 59 EC Treaty). In addition to the above mentioned rights, which are characterised by the fact that they are connected to an economic activity, it is furthermore guaranteed to everyone the right to reside in a country member different from his/her own, provided that the person can demonstrate to have the health service and sufficient support means. The citizen can, further, travel freely through each country of EU, provided with a simple passport or identity card without he/she is obliged to declare the reasons of his/her entry in the territory. The refuse that a member State can oppose to the access in its territory can be justified exclusively by reasons of public order, public security and public health.

The citizen who decides to remain in his/her country of origin claims specific rights contained in the EC Treaty. The European Union protects for example, the consumers and guarantees the right to purchase goods and services coming from other member States. Some rights have been provided for by the European Union also in favour of those who are not citizens of the Union. The relatives of the EU citizen, apart from his/her nationality, can accompany him/her in another member country and enjoy his/her same rights. The fundamental principles of the Community law extend also to the members of the European economic Space such as Liechtenstein, Norway and Iceland.

### *The Concept of Identity in the European Directive*

The European Directive 95/46/CE about data protection is aimed at giving to the data subject (owner of data) the most control possible on its own identity and personal data, posing a series of requirements on recipients, controllers, processors and even third parties. Art. 2, letter a), giving a definition of "personal data", says: "identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

The main principles behind the Data Protection Directive are:

- Personal data must always be processed fairly and lawfully
- Personal data must be collected for explicit and legitimate purposes and used accordingly
- Personal data must be relevant and not excessive in relation to the purpose for which they are processed
- Data that identify individuals must not be kept longer than necessary.

---

<sup>37</sup> Art. 9 Italian Civil Code.

<sup>38</sup> Art. 10 Italian Civil Code.

<sup>39</sup> Articles 2576, 2577, and 2590 Italian Civil Code.

- 
- Data must be accurate and, where necessary, kept up to date
  - Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them
  - Appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data
  - Personal data must not be transferred to a country or territory outside the European Economic Area unless that country ensures an "adequate level of protection" for data subjects.

#### *The European Convention for the Protection of Human Rights and Fundamental Freedoms*

The rule acknowledges to each person a right to his/her dignity, as well as a free development of "his/her" personality. This Convention has such a wide content to include the protection of different goods of the person and therefore also of the identity. In Art. 9 it is affirmed the person's right to "freedom of thought, conscience and religion", "to change his religion or belief" and to "manifest his religion or belief in worship, teaching, practice and observance". Art. 10 points out the right to freedom of expression including "to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." In affirming these freedoms, the need of man is reflected to be considered within the human sphere wherein he lives in consideration of his/her religious creed and his/her own ideological conviction. The privacy to Art. 8 is guaranteed, "Everyone has the right to respect for his private and family life, his home and his correspondence".

#### *The Concept of Identity in the Constitutions*

The person protected today by the Constitutions is very different from the "citizen" who is considered by the Constitutions of the liberal period. At the centre of the system protecting fundamental rights there is not the isolated individual, but the person considered in his/her social projection. Man and Woman are considered in their capacity of historically determined persons, plunged into the society, concrete persons who are considered in theirs historical and material existence, bearers of many needs and expectations.

The Constitutions have taken towards the fundamental rights of the persons some common orientations.

Among the aforesaid orientations, three acquisitions take a certain importance.<sup>40</sup>

- a) The first consists in the acknowledgement that there is an indivisible nexus and a direct connection between the guarantee of the person's rights and the Constitutions. This connections, clear and explicit in the first constitutional codifications of the liberal constitutional State<sup>41</sup>, remains in the most recent constitutional documents expressed by the most recent constitutional transitions. Therefore the task to guarantee the human person in his/her fundamental rights is entrusted to the constitutional systems.
- b) The second acquisition of the contemporaneous constitutionalism consists in the trend of the most recent constitutional documents to concretise and specify the concretely guaranteed subjective situations into a will of specification<sup>42</sup>.

---

<sup>40</sup> The reliability of this statement come from a study of the history of Constitutions, and an analysis of the difference between Constitutions.

<sup>41</sup> It is sufficient to consider the 1789 French Declaration of the Rights of Man and of the Citizen. The latter, after having identified preservation of man's natural and inalienable rights as the primary task of every political association, states that any society where such rights are not guaranteed has no constitution. Another example is the 1776 Declaration of Independence of the British colonies in North America, which recognised men as having innate rights – as is, in addition, the 1812 Constitution of Cadiz, which obliged the nation as such to preserve and protect all individuals' legitimate rights.

<sup>42</sup> As regards this tendency, it is sufficient to compare the schematic approach of the 1776 North American Declaration of Independence – "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain inalienable Rights, that among these are Life, Liberty, and the pursuit of Happiness..." – with the detailed listing of guaranteed rights contained, for example, in the Bills of Rights forming an integral part of the 1996 South African Constitution

The trend to specification does not represent a widening of the subjective positions which can be theoretically protected, but it proposes to codify a catalogue of the person's rights without gaps as well as it does not satisfy the need of didactical transparency so as to render the citizens informed and aware of their rights.

- c) Thirdly the modern Constitutions identify in the personalistic principle the standard value to be protected, on which the codifications of the single rights represent a historical specification of the subjective specifications, which deserve a particular acknowledgement. The constitutions try, in other words, to build around the human person considered in his/her integrity, a complex patchwork of rights.

The specification techniques of the person's rights are different in the various Constitutions. Some of them entrust this task to the ordinary legislator and to the jurisprudence, by limiting themselves to regulate in the Constitution text the freedoms and the rights considered "essential" and allowing their evolutionary interpretation through the presence of general clauses of the system opening, other, on the contrary, prefer to analytically detail the protected rights.<sup>43</sup>

### **Right to a Personal Identity**

The right to a personal identity is provided by some legislation through, e.g.:

- a) The right to expatriate and to change domicile.<sup>44</sup>
- b) The right to change the nationality or to give up one's nationality;<sup>45</sup>
- c) The right to change sex;<sup>46</sup>
- d) The right to change name;<sup>47</sup>

---

and of the Portuguese Constitution. Generally speaking, the tendency to detail and code rights emerges above all in constitutions formed at a time of political/institutional watersheds, as a response to the downfall of authoritarian regimes. This is true of (a) the European constitutions approved at the end of World War II, which marked the end of nazism and fascism (Germany, Italy, (b) Mediterranean constitutions born as a result of the downfall of authoritarian regimes (Greece, Spain, Portugal), (c) the constitutions of ex Soviet-block countries that have endowed themselves with new democratically-inspire orders and laws following the downfall of communist regimes (Poland, Hungary, Slovenia and Slovakia, and (d) the constitutions of Latin America and of new African states, always exposed to the risk of regression to coup d'état mode.

<sup>43</sup> The Italian Constitution – even although differing from the essentiality of constitutions in the liberal period and although undoubtedly a true constitution of a democratic, social and legally founded state – limits its codification of the individual's fundamental rights to just a few key liberties. There are historical reasons for this choice. And this is also evident in the constituents' determination to protect above all those liberties that, at that time, it seemed important to assert as a reaction to their violation during the fascist dictatorship. Examples are the attention given to regulating the ban on certain discriminations – freedom from arbitrary arrest; the inviolability of the home, communication and correspondence; the right of association, and the ban on censorship of expressions of opinion.

Conversely, the Spanish Constitution – developed and approved several decades later (1992) – contains a more detailed and complex structure of rights, which in turn contains greater specification of the catalogue of subjective positions explicitly recognised in the constitution. Examples are codification of the right to life and to physical and moral integrity (Article 15), to personal liberty (Article 17), to dignity, to individual and family privacy, and to one's image (Article 16) – and the statement that liberties connected with media have their limit in the right to dignity, privacy, image, and to protection of children and infants (Article 20) [cf. APPENDIX: "Spanish Constitution"].

<sup>44</sup> Italian Presidential Decree 396/2000; British declaration of Independence 1776; United States Expatriation Act of 1868.

<sup>45</sup> Art. 15 of the Universal declaration of Human Rights: "everyone has the right to a nationality. No one can be deprived of nationality unfairly or denied right to change nationality".

Nationality Law of the people's Republic of China no. 8 of 10 September 1980; British Nationality Act 1981; American Convention of Human Rights Art.20: "1. Every person has the right to a nationality. 2. Every person has the right to the nationality of the state in whose territory he was born if he does not have to any other nationality. 3. No one shall be arbitrarily deprived of his nationality or of the right to change it."

<sup>46</sup> Italian Law 164/1982, Swedish Law 1972, German Transsexuellengesetz, September 10th 1980; ÖStA Runderlass vom 10. Dezember 1981, Zl. 10.582/10-IV/4/81; The Dutch law (articles 29 through 29d of the Civil Code, law of April 24, 1985); Turkey Article 29 of the Civil Code, amended by Law No 3444 of 4 May 1988; The International Bill of Gender Rights (As adopted June 17, 1995 Houston, Texas, USA)

In the UK the Register of Births and Deaths cannot be altered to take account of gender reassignment surgery. The register is regarded as an historical document revealing historical facts and not current identity. Transsexuals have been bringing these issues before the courts for many years, so far unsuccessfully. Rather confusingly, however, it is the practice in the UK to allow transsexuals to change their name and gender on other official documents such as passports and driving licences (although when applying for insurance it is necessary for them to reveal their original gender).

<sup>47</sup> Italian Presidential Decree 396/2000 – only in given instances worthy of note (e.g., ridiculous or shameful names). California code of civil procedure section 1275-1279.6, and Family Code section 2080-2082.

- 
- e) The right to choose a pseudonym, nick name or artistic name, providing them with a certain degree of legal relevance and protection;
  - f) Punishment of the abuse of one's name or identity by third persons;<sup>48</sup>
  - g) Prohibition for state authorities to change forcefully identity attributes of a person;
  - h) Prohibition for parents to choose names that are not culturally or religiously rooted in the nation to which they belong;<sup>49</sup>
  - i) Prohibition for parents to choose names that are offensive of the (future) personality of children;<sup>50</sup>
  - j) Prohibition for parents to impose to all descendants the same name (or the same name as the father or mother);<sup>51</sup>
  - k) Prohibition for parents to impose names of a different gender than that of the born child.<sup>52</sup>

The right to a personal identity is limited by some legislation through, e.g.:

- a) Prohibition to expatriate without a state permission (Visa);
- b) The impossibility to give up citizenship;
- c) The impossibility to record the change of sex;
- d) Prohibition to change name under any circumstance;
- e) The obligation to change family name for the women, after marriage<sup>53</sup> or after divorce<sup>54</sup>.

### **Freedom from Physical Constriction (Habeas Corpus)**

The habeas corpus is indirectly relevant with respect to the rights of personality and identity. Rights of identity and personality would be of very little use if anybody would have the right to deprive us from using them by restricting our physical movements or our actions. Physical liberty is not only an expression of our personal freedom, but also of our right to a personality.

### **Inviolability of the Domicile and of the Privacy**

The right to privacy has been for a long time theorised as an extension of the inviolability of domicile<sup>55</sup>. The domicile has a primary place in the panorama of the fundamental rights of

---

<sup>48</sup> In Italy by Criminal Code articles 494-498 [cf. APPENDIX: "Italy – Criminal Code"].

<sup>49</sup> Sometimes these limitations were provided in order to protect the purity of a race or of a nation (fascist legislation, Law 13 July 1939 n. 1055; nazi legislation, Art. 13 of Law 5 January 1938 concerning the change of given names and surnames, and the second decree for the execution of the law regarding the change of the surnames and forenames of 7. August 1938). In other cases such limitations have been provided in order to strike a balance between the right to give a certain name to descendants and the right of the descendants to have a name that does not exclude them from a full integration in social and cultural life: for instance a name written in characters that are unknown in the grammar of the national language.

<sup>50</sup> Art. 58 Brazilian Civil Registration Act; Quebec Civil Code section 54. Quebec uses a Napoleonic Code-inspired civil code. Under the section "Assignment of Names," section 54, it says: "Where the name chosen by the father and mother contains an odd compound surname or odd given names which invite ridicule or which may discredit the child, the registrar of civil status may suggest to the parents that they change the child's name. If they refuse to do so, the registrar has authority to bring the dispute with the parents before the court and demand the assignment to the child of the surname of one of his parents or of two given names in common use, as the case may be."

<sup>51</sup> Italian Presidential Decree 396/2002. It is in fact forbidden to give a child the same name as his father if still alive, or as a brother or sister, or a surname as first name, or ridiculous or shameful names. The law in any case admits the possibility of changing ones first name or surname, via filing of a specific application with the Ministry of the Interior, but only in cases worthy of interest (for example: ridiculous or shameful names). In no case can applicants ask for attribution of surnames of historical importance or any case such as to mislead others as regards the applicant's membership of illustrious or particularly well-known families in the place where the applicant's birth certificate was issued or in his place of residence.

<sup>52</sup> Art. 35 Italian Presidential Decree 396/2000: "name must correspond to the sex".

<sup>53</sup> In Italy this has been regulated since 1975 by Article 141 of the Civil Code, later replaced by Article 143 of the Civil Code currently in force. This provides that a married woman maintains her maiden (i.e. family) name and that her husband's family name is merely placed after hers.

<sup>54</sup> Article 5 of Italian Law 898/1970 – with the sentence pronouncing the dissolution or cessation of the civil or lay effects of marriage (i.e. decree nisi), the woman loses the surname that she had added to her own after marriage. The court can, however, authorise the woman who makes a request in this respect, to retain her husband's surname, when this implies an interest of hers or of her children that merits attention.

<sup>55</sup> In the mid 19th century the Albertine Statute was promulgated, establishing the right to inviolability of domicile, inviolability of the right of ownership and, above all, in Article 32, recognising "the right to gather peacefully and unarmed, complying with the laws regulating exercise of the said right in the public interest".

freedom, as a spatial projection of the person, in the perspective to preserve from outer interferences behaviours kept in a determined background. This can be subject to limitations only in determined hypothesis provided for by the criminal law. The domicile violation, intended also as informational domicile, constitutes a criminal offence [cf. APPENDIX: "Section IV – Criminal offences against inviolability of domicile "].

### **Freedom of Speech<sup>56</sup> and Self Expression (the Protection of Reputation and Honour)**

The reputation is shaped as a distinctive essential sign addressed to represent the features, the physical aspect of the person, but also as expression, and the way to be of the personality in its complex. The right to a reputation as such is connected to the protection of reputation and privacy, intended as power to exclude others from the knowledge of facts concerning one's own person. Limits to this protection are: the consent of the person, the notoriety, the connection with events of public interest or which have taken place in public, the aims of the justice.

The right to honour, in the broadest sense, protects both the psychical sphere of the person, that is the sentiment of his/her own personal dignity (honour in a subjective sense) and the social consideration the person enjoys (reputation)<sup>57</sup>.

The contents of honour in subjective sense, since it is different in each person being a self-perception phenomenon, is protected with the recourse to the notions of the "equal social dignity" of all men<sup>58</sup>, the "free and respectable" existence<sup>59</sup>, of the "human dignity"<sup>60</sup>.

### **Freedom of Movement, to Expatriate and to Settle**

Each citizen is free, except for the legal obligations, to move or settle freely in any part of the national and community territory<sup>61</sup>, furthermore if he/she is provided with passport, he/she is free to leave the territory of the European Community and to re-enter. It is further guaranteed, at a constitutional level, among the fundamental freedoms, the domicile freedom (which is always

---

<sup>56</sup> It is the first freedom mentioned in the American First Amendment.

<sup>57</sup> Honour in the objective sense affects juridical capability. For example: when a guardian has to be chosen, the person chosen must be of impeccable conduct (Article 348 of the Italian Civil Code); alimony can be reduced if the conduct of the party receiving such alimony is reprehensible (Article 440 of the Civil Code); and a bankrupt cannot be appointed as a guardian (Article 350, no. 5, of the Civil Code).

Honour and moral integrity are also covered by criminal regulations (Articles 594 et seq. of the Italian Criminal Code); by the regulations of the so-called "Workers' Statute" (Italian Law no. 300/70) concerning remote control of employees, health checks, and investigations of opinions and facts not pertinent to appraisal of professional skills (Articles 4, 5, 6, and 8 of the aforesaid law); and also by the regulations envisaging the disciplinary power of professional orders over their members (Article 2229 of the Italian Civil Code).

<sup>58</sup> Art. 3 Italian Constitution; British legal system: "All human beings are born free and equal in dignity and rights, endowed with reason and conscience, and should act towards one another in a spirit of brotherhood"; Spain Constitution Article 14: "Spaniards are equal before the law, without any discrimination for reasons of birth, race, sex, religion, opinion, or any other personal or social condition or circumstance; China Constitution Article 33:" (1) All persons holding the nationality of the People's Republic of China are citizens of the People's Republic of China. (2) All citizens of the People's Republic of China are equal before the law. (3) Every citizen enjoys the rights and at the same time must perform the duties prescribed by the Constitution and the law.

<sup>59</sup> Art. 36 Italian Constitution; Spain Constitution Article 35: "(1) All Spaniards have the duty to work and the right to work, to the free election of profession or office career, to advancement through work, and to a sufficient remuneration to satisfy their needs and those of their family, while in no case can there be discrimination for reasons of sex. (2) The law shall regulate a statute for workers.

<sup>60</sup> Art. 41 Italian Constitution; Greek Constitution Article 2 co.: "Respect for and protection of human dignity constitute the primary obligation of the State."; Russia Article 2:"Humans, their rights and freedoms are the supreme value. It is a duty of the state to recognize, respect and protect the rights and liberties of humans and citizens."; Swiss Constitution Article 7:"Human dignity ought to be respected and protected"; Spain Constitution Article 10: "(1) The dignity of the person, the inviolable rights which are inherent, the free development of the personality, respect for the law and the rights of others, are the foundation of political order and social peace. (2) The norms relative to basic rights and liberties which are recognised by the Constitution shall be interpreted in conformity with the Universal Declaration of Human Rights and the international treaties and agreements on those matters ratified by Spain."

<sup>61</sup> Art. 16 Italian Constitution; Spain Constitution Article 19: "Spaniards have the right to freely select their residence and to travel in the national territory. They also have the right to enter and leave Spain freely under the conditions established by law. That right cannot be restricted because of political or ideological motives."

---

voluntary, except for the minors) and includes not only the house (residence) but also the place where the person carries on his/her job, as well as his/her occasional residence.

Freedom of movement is not only a physical freedom, it is also a moral freedom. It includes the right to a new start in life, which is almost equal to a new identity.

Even before data protection legislation, registrars of criminal offenders and of bankruptcies had limitations to their accessibility: the right to know the possible dangerousness of a person was postponed to his/her right to a fresh start<sup>62</sup>.

### **1.1.3 Identity from the Technical Perspective**

In technology speech, the term "ID" or "identifier" plays a big role rather than "identity"<sup>63</sup>. IDs denote "technological identities" of any possible object (or subject). An identifier could be a name, a serial number, or some other pointer or address to the entity being identified. Some identifiers allow unique mapping to a specific individual [Kent/Millett 2003]. Even if identifiers are not directly assigned to a user, but to, e.g., pieces of his/her hardware or programmes, the specific user may often be derived. Examples of identifiers are

- IDs for data sets, e.g., in relational databases where (unique) identifiers can be used to address data in a table or to join data of different tables;
- The MAC (Media Access Control) address which is a unique network card address and identifies the computer in a local area network, e.g., as an Ethernet address;
- The IP address which identifies the computer in the Internet;<sup>64</sup>
- Processor serial numbers (PSN), identifying, e.g., Intel's processors;<sup>65</sup>
- Globally unique identifiers (GUIDs), e.g., in Windows 98, Windows Media Player<sup>66</sup> or Real Player<sup>67</sup>;
- Cookies which are used to identify computers or users.<sup>68</sup>

Thus, those identifiers can be found in hardware (such as the PSN), in software (in applications such as the Real Player) or in services (such as cookies). In fact, today almost all computer-related device including chips or hard disks comprise identifying number.

For acting within an ICT system, the user has to be assigned an identifier. In many cases authentication, i.e., a verification of a claimed identity, of the user is necessary before any other action. In general there are three different methods for authentication [FIPS 1977]:

- "Something you know" (e.g., a secret such as a password),
- "Something you have" (e.g., a token or a chipcard) and
- "Something you are" (biometrics).

The processes of authentication and identification are distinct. Identification, seen from the technological perspective, associates an identifier with an individual without the requirement of a claim on the part of the subject. The objective of identification is to determine which identifier

---

<sup>62</sup> Decree 27. March 2000, n. 264.

<sup>63</sup> Although also called "digital identity", or to be more precise "digital partial identity", cf. Chapter 1.1.1.6.

<sup>64</sup> A correspondence table relates the IP address to the computer's physical MAC address on the LAN. The IP addresses used in the Internet have to be distinct, but proxies may assign dynamic IP addresses to requesting computers from an address pool or translate internal network addresses (not "official IP addresses" which are only visible within a LAN) into official IP addresses in the Internet.

<sup>65</sup> <http://www.intel.com/support/processors/pentiumiii/psqa.htm>.

<sup>66</sup> <http://www.microsoft.com/windows/windowsmedia/software/v8/privacy.aspx>.

<sup>67</sup> <http://www.real.com/products/player/g2/rsdata.html>.

<sup>68</sup> RFC2109 specification: <http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2109.html>.

refers to an individual. In contrast, authentication refers to the process of verifying the linkage between a (claimed) identifier and the individual [Kent/Millett 2003].

From the technical point of view pseudonyms can be seen as identifiers (cf. Chapter 1.5.2). Often there is a list of correspondences between pseudonyms and individuals (a look-up table) for unique mapping back to an individual, thus allowing the holder of the list to identify the action with the individual.

With respect to pseudonymous authentication by digital signatures, which prove the knowledge of a private key and thereby may authenticate a person, there are two forms of authentication: self-authentication and external authentication. Self-authentication means that a person links different own messages, e.g., by using the same digital pseudonym. External authentication means to link one's statement to an authorisation from others, e.g., by a certification authority [cf. Pfitzmann/Waidner/Pfitzmann 1990/2000].

## 1.2 Definition of Identity Management

### 1.2.1 Identity Management from the Sociological Perspective

In this text, we would like to introduce the term *Identity Management Applications* (IMA) for technical mechanisms for the administration of identities. The term *Identity Management System* (IMS) on the other hand shall be reserved for the whole ensemble of technologies and processes in which IMA are embedded among one another or within the social and technical infrastructure at large.

#### 1.2.1.1 Identity Management

After the previous elaborations we can define identity management one degree more precisely.

Identity management means recognition of situations and their valuation as "applicable to one self" (role taking) or forming them (role making). It would be better to use "Identities Management" when talking about supervising the different forms of possible participation in communication and to administrate them in a robust manner. In the end, one needs to correctly identify social situations and their relevant addressing options.

Identity Management, in other words, means to assess if and if so in which form a social system can be determined from the factually recognised form of communication or be initiated. If the type of social system has been recognised, role taking and role making regarding one self as "generalised other" commences. These decisions usually happen almost instantaneously without formal explication of attributes leading towards the decision. In meeting a childhood friend on the street, the context is sufficiently determined. If a colleague approaches a worker in an office space, most often with a fixating stare, formally correctly phrased sentences and a topic relating towards the organisational goal, this act puts the context of identity management beyond doubt as well. In the same way, there is also no doubt about the relation between a customer putting an order and the worker working on fulfilment of the order.<sup>69</sup>

Management of identity and identities is strongly supported by intuitively perceptible contexts. We move in spaces of civic administration, supermarkets, schools, offices, and shopping malls. In dealing with administration, shop keepers, educational institutions via the Internet through the browser on our home PC, the intuitive dimension is no longer available for recognition of the context and the determination of our relevant identity attributes. The "addressing" implicitly exerted in changing the context (by changing from one building to another, to another side of the street, by changing clothes, by showing a different look on one's face encouraging or

---

<sup>69</sup> In contrast to the distinction between identities management and identity management developed in the previous paragraph, we will use the term *identity management* as the broader term where the distinction is irrelevant.

---

discouraging the addressing of communication), needs to be explicated when using a letter, the telephone and, above all, the Internet.<sup>70</sup> People, place, situations, points in time, organisations, letters and faxes, e-mail, etc. all condense through the increasing use of computers and computer networks to explicit addresses. What hasn't been a large problem in practice up to now, namely control over or at least recognition of the change of context, identifying and appropriately defining and designing situations, archiving them and to robustly recall them, will become more problematic with mechanisation in the foreseeable future. In the course of mechanisation, implicit contextual knowledge is converted to addressing knowledge.<sup>71</sup> Forbidden rooms, e.g., office space of an organisation outside their customer premises, are out of bounds. This is a fact most people are intuitively aware of. One needs to be invited and usually escorted in order to gain the privilege of access. People generally know how physically close they may come to another person, which social distance is appropriate or inappropriate for which situation. All of these regulated forms of interaction need to be newly acquired and designed on the Internet.

Furthermore, the change of context, and especially a change of location and social situations, results in the fact that only a subset of the whole identity is being actualised per context. The linkage of events is only possible with a relevant effort. Generating linkage is, e.g., the business of private eyes. On the Internet, the situation changes, and one needs to take explicit precautions in order to only activate the relevant part in communication or in order not to disclose more than one is willing to.

The mechanisms for establishing trust can vary massively. In physical encounters, mutual assessments on whether or not to trust one another do run quickly and mostly subconsciously. If one already knows one another, technically spoken: has one already authenticated each other, one can build on the already available experience. If one doesn't know each other but moves in the defined context of an organisation and recognises each other in the typisation of function bearers, a contra-factual personal trust is created based on the underlying process and systemic trust. The same is true for trust in another person's reputation. Reputation is especially important in the context of writing. One believes an author to the degree he has made himself known and who has been stable and competently so over many years, and/or because he is employed by a trustworthy organisation and publishes with a trustworthy publisher.

A reason for trust is created when current knowledge or the possibilities for control and sanction have been exhausted, but expectations are constantly met [Luhmann 1989]. With regards to Internet communication, much communication is manifested in writing, where neither physis, nor reliable identity attributes, nor social context, nor another form of reputation for the initiation of measures to establish trust is available. Accordingly, one has to expect that the socially accepted model of trust were to change. Currently, Internet communication is being trusted solely because the only alternative would be "no participation in communication" in too many cases.

### **1.2.2 Identity Management from the Legal Perspective**

Identity management is not granted by legislation as such. This has three main reasons:

- a) The category is relevant principally in technological environment, in particular in open networks (Internet).
- b) Identity is not regulated organically by legislation, as it would be required in order to have a legal management of identities.
- c) Identity from a legal perspective has a dual function. Identification of the subjects and reference point for rights and obligations.

---

<sup>70</sup> The development of Uniform Resource Identifiers (URI) was only the beginning for a whole new set of considerations on technically supported address handling (<http://www.w3.org/Addressing/>).

<sup>71</sup> This is one factor in the success of Internet search engines. After a while of experimenting, people usually focus on one search engine only in order to pose (or post) their questions to the world.

Nonetheless legislation provides some (in most cases) constitutionally protected rights to individuals, that allow them to change some aspects of their identity, even if such changes are in conflict with the first function of the identity, which is to ensure uniqueness and identifiability of subjects.

The individual right to self-determination and self-expression (a fundamental aspect of the right of freedom) is more important than the need of the state to identify and make liable a person.

### **1.2.2.1 Right to a Name<sup>72</sup>**

Each person has foremost a right to have identification data (as we have seen in Chapter 1.1.2, the right to one's identification data is more important than the obligation to have them). So each person has the right to protect its own name and the right to avoid that it can be mixed up with that of others.

Constitutions protect the name<sup>73</sup> as an untouchable right of the person, and therefore nobody can be spoiled of its name as a form of legal punishment.

Legal systems allow to some extent identity management, as expression of the right to the name. The most known examples of name management are the cases when it is allowed to change one's name or family name (cf. Chapter 1.2.2.3).

### **1.2.2.2 Right to Move and to Change Domicile**

Considering that domicile is one of the elements that usually are used in order to identify a subject (cf. Chapter 1.1.2.1), the right to move and to change the domicile is an expression of the individual freedom. Again here the right to be free supersedes the need of the state to identify people and to make them liable.

This is antithetical to a reliable identification, because every change of the domicile makes legal persecution and any kind of legal responsibility more difficult to enforce. But obviously in

---

<sup>72</sup> The name has a long tradition. With the fall of the Roman Empire of the West the use of given names, surnames and nicknames were forgotten, and in late ages and in the early middle ages no name distinguished the families. Only around the 10<sup>th</sup> century, as a result of social and political changes, they were go back to the decision of the ancient Roman system of the use of the surnames. It was considered the best one and more reasoned system, in order to distinguish a person from any other having the same given name. So every noble and plebeian, free or enslaved, cultivators or craftsmen, took, beyond the baptism name, a last name.

But only in 15<sup>th</sup> century the use of surnames become effective. In some cases the surname derives from the name of the owned feud.

In Italy surnames were prerogative of rich families. In Venice on 13<sup>th</sup> century and the century following in other areas, even if with some resistance and delay, the use of surnames was extended to the less well-to-do layers of the population. But, only with the Council of Trento, 1564, it was imposed to priest to hold a tidy registry of the baptisms with name and surname, in order to avoid weddings between consanguineous.

<sup>73</sup> The name represents the distinctive legal sign of the person and constitutes the object of the relevant right. It consists of two appellations: the first name which is the individual appellation and the name which is the appellation common to his/her family group.

The right to name developed late in the history. In the Roman law it was in force the principle of the name changeability. Since the law made no distinction that a name pertaining to nobody or to another person was taken, it has to be considered that it was legal also the assumption of a name of another person [cf. Scialoja 1932]. It was very used to take the mother's name or the person from whom heritage was collected.

This regime was deemed to have a conclusion, in fact the public interest connected to the name did not fail to prevail. In fact the state needs to exactly identify its subjects, for many reasons which go from the repression of crimes to the tax management, to the draft. Therefore the idea broke through that it was necessary both the imposition and the conservation of the name, and, on the contrary, any possibility of arbitrary change was excluded (The Ordinance of Amboise, promulgated by Henry II on March 26th 1555 banned arbitrary changing of names, without a letter of dispensation).

Next to the public interest, the private interest stood: the individual has in fact the interest that no confusion takes place about his/her person with others, and such an interest shall not be prejudiced by the freedom of change.

In a particular way, the need appears to protect the interest of the class of tradesmen against the usurpation of the trade name (business name) as well as the necessity to avoid the usurpation of the titles of rank, frequent owing to the ambition to bear them. Subsequently this need extended to all social classes [cf. Ferrara 1941].

---

every liberal democratic system the right to move is granted to any citizen. This is not normal in authoritarian system and exactly for the reason that the freedom of movement makes law enforcement more difficult<sup>74</sup>.

It has to be remarked here, that in digital environment the relevance of the place of establishment has dramatically diminished. In fact (on-line) data availability makes very hard for a person to distance itself from them. Geographical movement of a person is not going to rebuild a new identity and a new life anymore (not to the extend it was before)<sup>75</sup>.

In this study we would like to point out that the loss of control on one's identity is not a necessitate consequence of technology. It is the consequence of the current way technology is marketed and designed (mostly through proprietary code, instead of open source code).

The utilisation of one's right of movement has not only practical consequences (in the most extreme cases the re-building of an identity, of a life) but also significant legal consequences<sup>76</sup>. Probably most apt way to recreate such possibilities in on-line human or legal relations, are Identity Management Systems. Otherwise the pervasive availability of data and the many tools able to profile us (it does not matter if complying to law, or violating it) will reduce our ability to choose how to present ourselves to the others and to decide what information about ourselves to disclose.

### 1.2.2.3 Right to Change Name<sup>77</sup>

The right to change name<sup>78</sup> is almost incompatible with the needs of personal identification, for this reason this right is limited to exceptional situations or to cases where the change of name happens for reasons that are considered of particular social value<sup>79</sup>.

---

<sup>74</sup> There is no need to reference specific legislation: in authoritarian systems citizens need a permission to move and/or have to register at police if they establish a new residence and/or need an exit visa if they want to leave the country. Probably the most striking form of lack of freedom, is when a person is not even allowed to leave.

<sup>75</sup> It has to be remembered that emigration, in particular to USA, took with it the need to "americanise" Arabic, Asiatic and often even European names, in order to "normalise" them to the American alphabet and to the spelling capabilities of the resident people. With the change of name something of the identity went lost, but a true fresh start was also the thereto related possibility.

<sup>76</sup> Change of nation, implies a change in applicable legislation. The change of residence implies a change in several applicable administrative competencies and regulations.

<sup>77</sup> The Munich Convention of 05/09/1980, which became executive in Italy with law no. 950 dated 19/11/84, establishes at clause 2 that "a person's surnames and names are decided by the law of the country of which the person is a citizen". Therefore, those situations that govern the surnames and names are evaluated according to the law of that country, if the person changes nationality, the law of the new country is applied.

California Code of Civil Procedure 1275-1279.

Michigan law permits an adult to change his/her name as long as the change is not done to escape creditors or to defraud someone. Under M.C.L. 71.1 the court will issue an order after being satisfied that there is no nefarious reason for the request. Only then can the name on the driver's licence or state identification card be changed through the Secretary of State's office. Change of gender designation can be requested at the same time even though Michigan law does not specifically address the issue of driver's licence or State ID.

Italian parents cannot give their children the mother's surname without undergoing the procedures laid down by clauses 84 and following of the Presidential Decree no. 396/00, except in the case when the natural child is first recognised by the mother and only later on by the father (clause 262 of the civil code).

The law governing the mother's surname is different in other European countries. In Germany the couple jointly decide on the family surname when they get married and in Spain the child is given a double surname, adding the mother's name to the fathers. There is then the French system, introduced by clause 43 of law no. 1372 dated 23rd December 1985, which, with the aim of reconciling the public right to establish the surname with the private need of being able to choose, the right (not obligation) has been introduced of being able to add the surname of the other parent to that of the father, but only as title of use without changing the mechanism whereby the legal name is given. This also takes into consideration the need not to lose economic *latus sensu* which could be granted to the maternal surname: a need which caused both France and Italy to allow a divorced woman to continue to use her husband's name.

In the USA, the problem regarding the choice of the surname, which is very flexible in both legal and administrative terms, is further attenuated by the fact that the child can change it once he becomes of age.

<sup>78</sup> The Ordinance of Amboise, promulgated by Henry II on March 26th 1555 banned arbitrary changing of names, without a letter of dispensation.

The 1794 decree of the French National Assembly forbade the use of names other than those shown in birth certificates. The 1844 Royal Patents of the Sardinian States prohibited name changes without sovereign consent.

The full identification of a person is almost impossible if at the same time one changes name and residence.<sup>80</sup> In the following cases there is specific legislation:

- Adoption;<sup>81</sup>
- Marriage and divorce;
- Change of nationality;<sup>82</sup>
- Change of gender;
- Ominous or offending names.

Changing the name by marriage is a remarkable exception. Clause 143 of the Civil Code establishes that the woman adds her husband's surname to her own, even though she continues to be known by her maiden surname in Civil Status certificates where the demographic data regarding the woman gives her maiden surname (clause 20 of Presidential Decree 223/89).

In some European countries, such as Germany, when a couple marries they can decide which surname to use, the husband's, the wife's or both. The chosen surname is the one by which they will be registered and is transmitted to their children. Therefore it can happen, in mixed marriages, that the husband, Italian, takes on his wife's surname and therefore their children are registered under it. This is contrary to legislation, whereby legitimate children take on the father's surname and an Italian citizen can only change his generalities with a specific procedure established by law. In this case, the hypothesis of changing the surname does not exist in the real sense of the word, as it does not derive from a court order, which, perhaps, could also be recognised in Italy, but from an administrative measure that cannot be acknowledged. In this case, name change is irrelevant for an Italian citizen and the children's birth certificates, once they are registered, would have to be rectified and the paternal surname added.

#### **1.2.2.4 Right to Dress and Decide the Personal Outlook**

The freedom of clothing is comprised in the freedom of expression of the individual. Each individual is free to wear what suits him or her, provided that this does not infringe the good costume or the public order. Again, this is not only a physical freedom. This means that each of us has the freedom to decide the look, the semantic content of its own identity. The ability of others, even of the State or of law enforcement agencies, to recognise us is never a limitation to our right to self-determine our look.

There are very few exceptions, like in case of public manifestations or gathering of huge crowds (like football, baseball, soccer games), where some criminal legislation prohibits participants to cover their face with scarves or to wear helmets.

<sup>79</sup> It has to be remarked that when identification was carried out through appurtenance to a clan or family, the use of the right to move was equivalent to the loss of identity. Only since when there are reliable administrative records tracking individual identity, the move from one location to another is not at the same time a more or less complete loss of identity. At that time the right to move was strongly limited (if not excluded at all) for most people.

<sup>80</sup> Currently the EU is experiencing the daunting task to identify people trying to establish illegally their living residence in Europe in order to have a chance to work and live in better human conditions.

<sup>81</sup> Italian law establishes two "types of adoption for juveniles": (1) – legitimate adoption (2) – adoption in special cases which are governed by the special law no. 184 issued in 1983. There is also adoption for "adults" which is governed by the Civil Code. In the first case, the adopted child loses its original surname and takes on that of the adoptive parents. In the second case and in the case of adoption of "adults", the surname is established in accordance with clause 299 of the Civil Code, about which the Ministry of Justice issued a circular with its opinion of the interpretation.

<sup>82</sup> In truth, a "Foreign Citizen" who takes on Italian citizenship does not change his surname, but keeps the one given at birth. However it could happen that a change in surname that took place before naturalisation could not be acknowledged by Italian legislation.

For example, in many countries, the woman takes on her husband's surname to all effects and it is always used in all identification and travelling documents. If the woman takes on Italian citizenship, she would then be known by her maiden surname, in accordance with Italian law and the way a married Italian woman is recognised.

The above in consideration of the fact that the above mentioned Munich convention establishes that by changing nationality, the law of the new country of citizenship is applied. Therefore in certain cases, the change of citizenship could also involve the change of surname.

---

### 1.2.2.5 Right to Have a Pseudonym<sup>83</sup>

The right to pseudonymity can be defined as the right not to disclose that we don't want to disclose our identity. This is at least the case with pseudonyms which look like real names and don't reveal that they are pseudonyms.

In legal systems of democratic liberal societies there is a general rule: everything that is not forbidden is allowed. The right to freedom is unlimited, as far as legislation, the rights of third persons or the moral code are not providing such limitations<sup>84</sup>. Article 6 of the European Charter of Fundamental Rights declares that "Everyone has the right to liberty and security of person".

Most of the European constitutions have such clauses too. For example the German Grundgesetz says in Article 2 paragraph 1: "Everyone has the right to the free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral code".<sup>85</sup> The France Declaration of the Rights of Man of 1789 declares in article 4: "Liberty consists in the freedom to do everything which injures no one else; hence the exercise of the natural rights of each man has no limits except those which assure to the other members of the society the enjoyment of the same rights. These limits can only be determined by law".<sup>86</sup> Therefore there are several articles of the Italian Constitution that affirm the inviolability of different aspects of individual freedom: "Personal liberty is inviolable" (Article 13) and "Liberty and secrecy of correspondence and other forms of communication are inviolable" (Article 15).

Given that a Constitution recognises the individual freedom and that only legislation can curb or limit individual freedom, the right to pseudonymity requires simply that the legal system:

- 1) Is not prohibiting or punishing the use of a imaginary name or of the name of another (determined or undetermined) person *as such*.
- 2) Is not requiring people to carry with themselves always identification tools (identity cards, passport etc.) and/or to disclose one's true identity on demand.

On the contrary there is no right to pseudonymity if the legal system is punishing the use of a pseudonym *as such* or if there is a general requirement to be identifiable.<sup>87</sup>

The Directive on Electronic Signatures 1999/93 expressly recognises the right to pseudonymity in recital 25<sup>88</sup>, Article 8, Section 3<sup>89</sup> and letter c) of Annex I<sup>90</sup>.

---

<sup>83</sup> The pseudonym is an accessory element of the identity. In Italy within the range it is taken by the person, it serves to designate him/her, to distinguish him/her from the other, generally with a greater efficacy (artistic or literary pseudonym). When it has acquired the importance of the name, it enjoys of its same protection. It is therefore an additional element of identification of the person, a reason for which, when it takes the importance of the name, it enjoys its same protection.

The pseudonym, also according to the Directive 1999/93/EC about the e-commerce is considered equal to the name. In Art. 3 of the enclosure 1 it is stated: "Without prejudice to the juridical effects that the national legislation attributes to pseudonyms, the member States do not prohibit to the certification service supplier to mention on the certificate a pseudonym at the place of the name of the signatory". Furthermore it gives the possibility to include in the certificate the pseudonym at the place of the name: "The qualified certificates shall include: the name of the signatory of the certificate or a pseudonym identified as such".

<sup>84</sup> The model of such concept of freedom is the American Constitution, that has been taken as a model by most of the European constitutions of the second half of the 20<sup>th</sup> century.

<sup>85</sup> "Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsgemäße Ordnung oder das Sittengesetz verstößt."

<sup>86</sup> La Déclaration des Droits de l'Homme et du Citoyen: "Article 4 - La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui: ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits Ces bornes ne peuvent être déterminées que par la loi".

<sup>87</sup> In Italy a pseudonym cannot be used in the case of buying property or forming a company, as identification by a Notary is required. Neither is it allowed in the case of renting property, because the lessee, as per law no. 15 of 6th February 1980, must ask for the tenant's documents and must inform the local police of his details. The same is valid in Italy when staying in hotels, as per Ministerial Decree 12<sup>th</sup> July 1996.

<sup>88</sup> Recital 25 provides: "Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law".

Such recognition of the need of pseudonymity is very relevant. Its ratio is that in the information society (and in particular in open networks) a good identification and authentication, are at odds with the right of privacy.

It is maybe ironic that strong cryptography (qualified signatures) are a perfect identification tool, because even if we don't know the real name of the other party, we are able to verify unmistakably again and again if we are dealing with the same person.

So in order to identify a person in open networks, technically (and legally) speaking we don't need anymore to know a name or an address. With the permission of the interested person we can connect the story of our relation to a reliable unique identifier (the pseudonym or the number of the signature certificate).

Technically and legally speaking, after the idea of the Directive on Electronic Signatures, which expressly declares the possibility of using pseudonyms, we can lawfully have different identities for on-line relations we establish – hence the urgent need for IMS. Recital 25 and letter c) of Annex I of the Directive on Electronic Signatures recognise the right to pseudonymity from the perspective of the European legislation. Still Member States have the sovereignty of to require the identification of holders of Certificates for any reason compatible with their constitutions or legal systems. The legal sense of letter c) of Annex I, anyway, is that as far as national legislation allows it, the user of a Qualified Certificate has the right (in the full sense) to require and obtain a Secure Signature Creation Device that does not disclose his/her full identity.

So far some Certification Authorities issuing Qualified Certificates are organised in order to issue such pseudonym certificates. In Italy none of the Certification Authorities is able to issue pseudonym certificates. In Germany the Signaturgesetz and the Signaturverordnung commit German Certification Authorities to provide the facility of using a pseudonym certificates (cf. § 5 paragraph 3 SigG).

Currently the protections of national constitutions are not applied by the legislator or by jurisprudence at the digital environment. So we can have legislations, like that of the United Kingdom, that provides the absolute right not to carry identification papers in the physical world, but limits strongly the individual rights in the digital environment, even devoting individuals of the freedom not to impeach themselves (in full breach of any international convention on Human rights).

The European Convention of Human Rights, that has also been accepted by the United Kingdom, will be a great opportunity to reaffirm the individual rights also in the digital environment. In fact it is not the lack of identification, but the non-existence of a technically safe digital environment in which go opt-in that makes the digital environment dangerous. The Middle Age and the time of absolute monarchies have proved the uselessness of harsh limitations to individual freedom. Social peace and public order have greatly improved, since individual rights are granted by legislation. The same will be in the digital environment as far as some trustworthy technology or infrastructure will be available.

---

<sup>89</sup> That provides "Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name".

<sup>90</sup> That provides that a Qualified Certificate shall contain "(c) the name of the signatory or a pseudonym, which shall be identified as such".

---

### 1.2.2.6

### Right to be Left Alone (Privacy Protection<sup>91</sup>) and Right of Anonymity

The right to privacy comprises the right not to disclose information and the obligation for data processing parties to provide technological and organisational measures to protect disclosed personal data.<sup>92</sup>

So the data gathering as such is not prohibited, but in order to collect personal data lawfully, there is the obligation to inform the interested person (and the data protection authority). Data minimisation is the key approach of legal systems recognising an individual right to data protection<sup>93</sup>.

The current problem is that data minimisation is an approach difficult to enforce: it is more difficult to select relevant data than to store everything that could be of interest. Storage capability is no more a limiting factor: huge databases and storage devices have become dramatically cheaper in the last 10 years.

The difficulty to enforce a proper gathering and handling of personal data is the reason why there is an increasing interest in Identity Management Systems.

The problem of properly implementing on-line identity has been technically solved: There is the possibility to use the electronic signature for mutual identification and authentication.<sup>94</sup> The problems related to the identification through a terminal or a random telecommunication link, can be solved through cryptographic tools, instead with IP addresses or other inappropriate substitutes.

Up to now pseudonymity or anonymity were the only viable options for on-line interaction. A reliable identification needed always at least some kind of direct or indirect personal contact. This is not anymore true: Many kinds of electronic signatures are available so that legally speaking there are the following options practicable:

- a) To be fully recognisable through qualified certificates, according to the Annex I of the Directive on Electronic Signatures 93/1999 EU;
- b) To be recognisable through a pseudonym displayed on the qualified certificate, according to the Annex I of the Directive on Electronic Signatures 93/1999 EU;
- c) To self declare one's identity;
- d) Not to declare one's identity.

From a situation where identity verification was costly and often unreliable and only options 3 and 4 where available, the digital world has obtained a legal and technical possibility

---

<sup>91</sup> Many Constitutions contains references to privacy protection, particularly the recent constitutions of East Europe [cf. APPENDIX: "Constitutions references to privacy protection"].

The right to privacy was theorised for the first time in the United States at the end of 1800. In its traditional meaning, the right is intended as the right to be left alone, that is the right to the privacy of his/her private sphere. Warren and Brandeis, authors of the essay "The right to privacy", condensed with the formula "the right to be left alone" the aspiration of the individual that his/her private and personal sphere is protected from interference by other people, both public and private, by emphasising the intangible value of the man in the different aspects of the individual and social life [cf. Warren/Brandeis 1890]. In the intention of the paper's authors the right to privacy signified "the right to enjoy life, or the right to be let alone" – a right threatened, and sometimes suffocated, by intrusions into the sphere of private life in a society dominated by the need for news and information and under the control of mass media.

<sup>92</sup> In Italy it is possible not to give the civil status or profession in the identity card, while in Austria and Germany there is the chance of not changing surname in case of marriage, to respect the right of not making the name of the person to whom one is married known.

<sup>93</sup> Just consider the case of abandoned children, who in the past were identified as children of N.N.

<sup>94</sup> From the technological point of view, digital signatures can not directly identify or authenticate persons. In the case of electronic signatures, there is often a fictitious presumption of a (mostly unique) linkage to a person known by a Certification Authority.

unavailable in the physical world: the identification without disclosure of any personal information. This new possibility will drive technological and legal evolution in the next years.

### **1.2.2.7 Right to Change Gender**

The right to change gender constitutes the extreme expression of freedom of the individual. It can be considered as an aspect of the freedom of expression, constitutionally protected, since it is a way to express his/her personality.

In many systems the principle of the gender unchangeability has failed. The artificial change of the sex can take place if it satisfies an interest objectively and subjectively intended of the person, for the purposes of the development of his/her personality and in the substantial respect of his/her dignity.<sup>95</sup>

As a confirmation of the foregoing, the transsexual has the possibility to change name. Only a few democratic liberal legal systems do not recognise change of gender, because of alleged violation of decency and moral.

### **1.2.2.8 Right of Honour<sup>96</sup>**

From the perspective of identity management the protection of honour is relevant considering the following situations:

- a) The right to change the name because the given name (Mario Rossi, Hans Meier) is not sufficiently identifying in itself;
- b) The right to change the name because the name includes a negative dishonourable adjective or significance or because it is the name that is related to negative persons, criminals and so on (Jack the Ripper, Adolf Hitler, Joseph Stalin).

In these cases legal system can provide the right to change the name.

From a more general perspective, we have a further confirmation of the relevance of honour related to identity management and to the civil and penal law regulations if we consider that:

- Honour is protected by criminal legislation [cf. APPENDIX: "Crime against honour"]<sup>97</sup>
- Honour is recognised by many constitutions<sup>98</sup>
- In some legal systems the self defence/enforcement of the honour is admitted<sup>99</sup>

---

<sup>95</sup> Art. 32 Italian Constitution; Spain Constitution Article 25: "(1) The right of human beings as individuals and as members of the social body are guaranteed by the State, all the functionaries whereof are obliged to safeguard the unimpaired exercise thereof. (2) The recognition and protection of the fundamental and inalienable rights of man by the State shall aim at achieving social progress in freedom and justice. (3) Abuse of rights shall be prohibited. (4) The State has the right to demand of all citizens that they perform the duty of social and national solidarity."

<sup>96</sup> Honour can be explained as the everlasting, everyone appertaining right that is the result of the dignity of man. In the intendment of § 16 ABGB (Austrian Civil Code) the sense of honour of an individual person, who believes that its pride was hurt is not considered as such. Necessary is the general understanding of defamatory matters. The Austrian High Court of Justice draws because of § 16, 1330 ABGB (Austrian Civil Code), § 7 UWG (Competition Law) and the §§ 111-115 StGB (Criminal Law) that honour deserves an absolute protection against defamatory matters.

<sup>97</sup> In Italy "crimes against honour" are slander and libel (listed by clauses 594-595-596-597-598-599 of the Penal Code): slander is the offence to the honour and the decorum of a person who is present and involves imprisonment between 2 and 6 years: if the offended person is absent, then the crime of "libel" arises, clause 595 penal code, when accused by the offended person, and the fact is aggravated if committed in the press or by other public means. There are also crimes against family moral: incest and attempts against family moral through the press if a "public scandal" thus derives [cf. APPENDIX: "Crime against honour"].

<sup>98</sup> The Constitution of China protect honour:

Article 101: "Citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited."

Article 102: "Citizens and legal persons shall enjoy the right of honour. It shall be prohibited to unlawfully divest citizens and legal persons of their honorary titles."

- 
- In some legal systems honour has a reflection on legal capability<sup>100</sup>

It is possible to conclude that legislation in general (not only allows, but even) favours the self-protection of honour as far as it is realised through lawful means and without the use of force or violence.

### 1.2.3 Identity Management from the Technical Perspective

As technical identities simply are numbers, which can represent any object, they may identify directly or indirectly an individual, an organisation, or a machine.

It is relevant from the privacy perspective that even if those identifiers do not directly represent an individual, but only a specific device, frequently there is a relation to a person so that many of these identities have to be regarded as at least potentially personal data. But as the existence and the disclosure of those IDs often goes unnoticed by the users, managing them is quite difficult: In many cases technology does not provide the functionality to influence assignment, storage and disclosure of those IDs. Only when a sufficiently large numbers of users became aware of privacy threats, some software and hardware manufacturers who implemented GUIDs in their systems reacted by informing the user and offering the possibility to delete the ID or to control its disclosure.<sup>101</sup> A possibility to regain control over these IDs is offered by some anonymising services which help the users in substituting or deleting those identifiers.<sup>102</sup>

In general it is not possible to successfully manage one's partial identities without knowing when and where they may be involuntarily disclosed. This is not only the case with data trails in digital networks, but also capturing biometrics, e.g., by video surveillance, is often possible without knowledge and consent of the individual.<sup>103</sup> Whereas the user can blur identifying data by anonymising services, there is no equivalent solution for preventing others to capture publicly noticeable biometrics such as the face, the shape of the body or the way of walking. Identity Management Systems as described in this study are acting as gateways and guardians for users in digital networks, but cannot prevent undesired data collection outside the network.

Considering the three main methods of authentication (cf. Chapter 1.1.3), managing digital identities has to be realised in different ways:

- For "something you know": The secrets which serve as authentication of a partial identity can be handled within the IMA through their whole lifecycle (including generation). The IMA may implement a single sign-on function.

---

<sup>99</sup> Articles 340 and 98 of the Jordanian Penal Code exempt or reduce the punishment of individuals convicted of murdering women in the name of honour. Articles 340 (a) exempts from punishment a perpetrator who discovers his wife, or one of his female relatives, committing adultery with another person, and kills, injures, or harms one or both of them.

Article 340 (b) reduces the sentence for the perpetrator of a murder, injury, or harm, if he discovers his wife, one of his sisters, or other relatives, with another man in an illegitimate bed.

And Article 98 reduces the sentence for the perpetrator of a fit of fury crime committed in response to a wrongful and serious act on the part of the victim.

In Italy, law 442/1981 has repealed crimes committed for "motives of honour". This involved cases which, for the element of "offence to personal or family honour", constituted "minor" crimes and were therefore sanctioned with reduced sentences. Among these cases were: "murder for motives of honour" (clause 587 penal code), "infanticide for motives of honour" (clause 592 penal code). Motive of honour was also recognised as an attenuating circumstance in the case of personal injury and premeditated murder by clause 587 penal code, paragraph 2, and as justification for the crime of assault and battery.

<sup>100</sup> According to Italian civil code, when a guardian is chosen, a person of exemplary behaviour must be chosen (clause 348 civil code) and a bankrupt cannot be named guardian (clause 350, no. 5 civil code).

<sup>101</sup> E.g., <http://www.microsoft.com/windows/windowsmedia/software/v8/privacy.aspx> or <http://www.realnetworks.com/company/privacy/realone.html>.

<sup>102</sup> E.g., cookie managers.

<sup>103</sup> From the privacy point of view biometric techniques which do not require an active participation of the individual should not be used [Hes/Hooghiemstra/Borking 1999].

- For "something you have": Certificates can be stored within the IMA. If we think of IMA which can access hardware tokens for authentication, a support is possible. We can imagine a solution where the IMA acts as a "jukebox" for all tokens like chipcards, choosing the device appropriate for the situation. But normally not the whole lifecycle of authentication identity can be handled by the IMA, e.g., issuance and distribution (and in most cases also revocation) of chipcards need physical contact or delivery channels outside the digital network.
- For "something you are": With biometrics, even more channels outside the digital network and thereby outside the direct controllability of the IMA exist. In general, the IMA could not serve as a guardian between the individual and the device capturing biometric data. The user is left alone with managing biometric properties and possible capturing by sensors.<sup>104</sup>

In all cases IMA can manage the data flow after authentication (thus forming a partial identity) as far it is handled in the network. Moreover, they can help in asserting privacy rights, asking for privacy policies, requiring access etc.

## 1.3 Definition of Identity Management System

### 1.3.1 IMS from the Sociological Perspective

On the level of an Identity Management System (IMS), we notice that every user using an IMA could be perceived as a – possibly threatening – "data processing entity" that needs to be effectively countered by use of an IMA.

The term "Identity Management System" (IMS) should describe the infrastructure in which Identity Management Applications as components are co-ordinated.

In order to ensure functioning identity management in such a fashion that it will find general acceptance with users, we believe that an Identity Management Protocol (IMP) needs to be defined that enables transmission of the type of desired communication (or social situation), so that the class of pseudonyms to be used can be determined automatically on the sender and the receiver side. We believe that the development of an IMP is mandatory because an IMP would relatively easily allow a usable, implicit interpretation of various classes of communication, i.e., activation of sub-identities.

Nonetheless, in order to maintain an appropriate level of data security and date protection, it is of course indispensable to leave the user's capability intact to explicate implicit aspects of communication at any time. This results in a requirement for giving access to sets of rules and possibly program code.

An IMS, according to this specification, denotes an infrastructure within one or between several organisations, which have agreed upon a mutual model of trust in managing and using identities. Moreover, IMS can also denote an implementation of identity management encompassing a whole society.

An IMS can only take hold across a society if it is in line with the structure of social systems. This means that implementation as well as use of systems needs to be economically calculable, politically acceptable, legally compliant and scientifically controllable.

In addition, IMS relies on a technical infrastructure enabling the handling of digital signatures for authentication and the self-evident use of anonymous communication. It is much less a technical question than a legal and political one, in how far access to attributes of a digital identity is granted to an organisation or the user.

---

<sup>104</sup> In principle it is possible that biometric or other sensors "inform" the IMA on their data processing procedures, enabling the user to take appropriate actions. But sensors without this transparency functionality cannot be prevented.

---

As required by law, a society-wide implemented IMS has to be of state-of-the-art design regarding legal aspects as well as aspects of data security technology and privacy protection technology – insofar it would be a "Privacy-Enhancing Identity Management System". Admittedly, there is a risk that companies, which offer and use IMA at an early stage, create fait-accomplish, as legal and political counteracting mechanisms react comparably slow, so that the outcome would not necessarily be privacy-enhancing or at least privacy-compliant.

### **1.3.2     IMS from the Legal Perspective**

All the examples described in Chapter 1.2.2 are significant in order to understand for what perspective and for what purpose the legislation considers identity and the changes to a given identity. But in particular we would like to refer to Subsections 1.2.2.2, 1.2.2.5, and 1.2.2.6 (Right of movement, right of pseudonymity, right of privacy).

The legal assessment of technical tools to manage personal identity will be carried out in Chapter 4. In fact there is not already a definite legal dimension for Identity Management Systems beside that they have to comply in Europe to the European legislation. In the description of the use cases and of the visionary scenarios this study will try to make also some forecasts on what legal problems and regulations will be likely or useful.

### **1.3.3     IMS from the Technical Perspective**

The roots of identity management in digital communication are about 30 years old. First ideas of a multi-purpose identity management are mentioned by David Chaum 1984 who wanted to give each individual a card-computer to handle all payments and other transactions [cf. Chaum 1984]. Pseudonyms with various properties are the core concept of this card-computer aiming for privacy enhancement. He had written about an Identity Management Application, which already was in fact a "privacy-enhancing Identity Management Application". Since then and in particular in the last two years a lot of definitions of identity management from different points of view were generated.

David Chaum defined identity management (respectively "the new approach") by "three major differences" [cf. Chaum 1984]. The first is in the use of identifying information: "Under the new approach, an individual uses a different account number or 'digital pseudonym' with each organisation. No other identifying information is used." He sees a second difference in whose mechanism is used to conduct transactions: "With the new approach, an individual conducts transactions using a personal 'card computer.' This might resemble a credit-card-sized calculator and include a character display, a keyboard, and a short-range communication capability (...)." The third defining difference in his opinion is in the kind of security provided: "... the new approach allows all parties to protect their own interests. It relies both on individuals' card computers withholding secret keys from organisations and on organisations' computers devising other secret keys that are withheld from individuals. During transactions, the parties use these keys to form specially coded confirmations of transaction details, the exchange of which yields evidence sufficient to resolve errors and disputes".

This definition emphasises the inception of the relationship between user and organisation utilising a certain address, a pseudonym. From a functional perspective, the use of pseudonyms has the advantage that it absorbs and collapses the type of relationship into a single identifier, the pseudonym. It is entirely possible that by finding a suitable pseudonym, the whole kind of relationship and thus the requirements for identity attributes have already been solved. A pseudonym functions as an internally and externally accessible denominator for a certain sub-identity (internal view) or especially tailored identity (external view) at the same time. From a data privacy perspective, a transactional pseudonym offers the additional advantage of rendering linkage with other identity attributes more difficult or inhibiting it altogether. Furthermore, use of a pseudonym makes attribution of a communication to a certain person more difficult or impossible, who would then serve as an anchor point for the attribution of identity attributes. In

other words, in many cases the use of a pseudonym allows exertion of the right to informational self-determination, because it contains an implicit opt-in mechanism through its built-in option for self-disclosure.

A "card computer" would today be seen as a Personal Digital Assistant (PDA) that a person is constantly wearing, or, on the Internet, a Personal Agent (PA). The fulfilment of enormous security requirements would be a prerequisite for the use of these technical media for management of identities. The third aspect therefore emphasises the requirement that security with regards to fault correction and disputes needs to be ensured. Last not least, this definition emphasises that the typical area of use would be in the relationship between users and organisations. IMA do only play a limited role in interactional systems, at least in the current state of development of these systems. In a possible future, where use of IMA is ubiquitous, it could be part of the definition of a friendship or an intimate relationship to not manage these relationships with an IMA.

There are some user-oriented definitions of identity management [cf. Köhntopp 2000; Dyson 2002a; Jendricke 2002]. A very impressive slogan characterise privacy-enhancing identity management: "Make the user owner of her profile." [Koch 2002] In contrast hereto, some definitions point out an intelligent user administration's aspect of avoiding transportation cost in heterogeneous environment [cf. RSA Security<sup>105</sup>; M-Tech<sup>106</sup>] or link identity management to personal agents or machine agents [cf. W3C<sup>107</sup>] or narrowly restricted on business processes [cf. Sun<sup>108</sup>; Dumortier 2002].

The roadmap of the RAPID Project defines identity management with the basic requirements of a digital identity solution: "To ensure successful identity management, a digital identity solution should support at least the following basic requirements. Reliability and dependability (...) Controlled information disclosure (...) Mobility support". And later: "An identity management solution can help you get users, systems and applications on-line and productive fast, reduce costs and maximise return on investment. This solution can automate and simplify the management of user identities, access rights and privacy policies across the e-Business infrastructure. To effectively manage internal users as well as an increasing number of customers and partners provides the only integrated solution that addresses all four key areas of identity management: Identity lifecycle management (user self-care, enrolment and provisioning); Identity control (access and privacy control, Single Sign-on and auditing); Identity federation (sharing user authentication and attribute information between trusted Web services applications); Identity foundation (directory and workflow). A scalable identity management solution also supports open standards, which can speed deployment and help reduce costs" [cf. Huizinga 2002].

This definition addresses all relevant aspects an IMA or an IMS need to fulfil. The economic efficiency of a universal user and resource administration that would be possible via an all-encompassing IMS is emphasised as a functionally important aspect.

David Birch, Director of Consult Hyperion, has published several articles about identity management and digital identity. His definitions are motivated by the problem of identity theft, which should be solved by security mechanisms within Identity Management Systems: "Overall, a well-executed identity management strategy should result in increased security. At the operational level, this is because a proper implementation of that strategy will mean that all e-mail, all web access and other services will be using digital identities and the digital signature services that they allow." [cf. Birch 2002: 4]

---

<sup>105</sup> <http://www.rsasecurity.com/products/>.

<sup>106</sup> [http://www.psych.com/docs/what\\_is\\_id\\_mgmt\\_2.pdf](http://www.psych.com/docs/what_is_id_mgmt_2.pdf).

<sup>107</sup> <http://www.w3.org/2001/03/WSWS-popapaper57>.

<sup>108</sup> [http://www.sun.com/software/sunone/wp-identity\\_mngt.pdf](http://www.sun.com/software/sunone/wp-identity_mngt.pdf).

---

In the following, we want to try to develop a definition of technically supported management of identity or identities taking into account the general considerations from previous Chapters as well as such aspects that have not been addressed to strongly in the aforementioned definitions.

A technically supported identity management has to empower the user to recognise different kinds of communication or social situations and to assess them with regards to their relevance, functionality and their security and privacy risk in order to find an adequate role making/role taking.

### **1.3.4 Multi-purpose Identity Management Application**

An Identity Management Application needs to administrate the explicit determinations or changes of contexts in the form of addresses and layered, granular authentication and access privileges for the user. The means therefore are, among others, passwords and signatures (authentication), credentials (showing authorisations without linkability), pseudonyms (in the sense of addresses for granular, situation-conformant identity attributes protecting against linkage) and archiving functions for administration of communication history. It should allow managing an arbitrary social relationship over an arbitrary period of time. Furthermore, it needs to give the user means for constructing an encompassing digital identity and partial identities for specific communication requirements, especially with organisations (from business, state, communes, science).

In order to reduce the complexity of requirements, a kind of "balancing" between the different mechanisms seems to be a feasible approach. An IMA in a web of trust could, e.g., ensure as a trustee that the reputation of the trustee compensates the absence of reputation of a user for transacting a risky business, e.g., giving credit. As a result, there is a need for an extraordinary relationship of trust between the user and the reputation-"donating" trustee organisation. Trustworthiness could, e.g., be proven for an organisation by giving the organisation complete access to one's digital identity. This is precisely the approach chosen by Microsoft Passport, but traditionally, the state demands the same right, and it could also be implemented by freely selectable "communities of trust".

Multi-purpose identity management means managing a number of social situations. If only one particular social situation, e.g., shopping, is being supported by an Identity Management Application, the latter could be called a single-purpose Identity Management Application. If a single-purpose Identity Management Application would be used in almost all different contexts of technology-based communication, it would be an all-purpose Identity Management Application. Remarkably, one context (e.g., the area of e-Health) includes several sub-contexts, which may have their own multi-purpose requirements: inspection of a medical record, consent to an X-ray or operation, ordering of drugs.

According to the point of view of this study, a typical multi-purpose identity-management-application is equivalent to a system in which the user is allowed to choose a general but particular social context and their own role within it (e.g., patient, customer, citizen, scientific expert in exactly this context) and the processing of the requirements of the corresponding specific communication is being supported in a decisive manner by the application. This support could exist in the possibility to choose anonymously from a variety of information, or to vote for a political party, order a product or publish a scientific essay by use of a pseudonym.

In this sense, a single sign-on application could indeed be called a multi-purpose application. It allows central deployment for a variety of purposes, e.g., sign-in processes in e-Government or e-Commerce, as well as a theoretically possible management of several pseudonyms for one user. Furthermore, it will surely be helpful concerning the right choice of context. It would "only" require an on-line connection for every technology-based communication.

Another aspect is the integration of IMS functionality in existing ICT. We can think of specific "Identity Managers" which act as a universal application, managing the user's identities, or the

IMA could only be an interface, a proxy or a gateway, communicating with multiple other applications. In contrast to those more general approaches which could also be used for many or all purposes, application-specific IMA, e.g., in form of a plug-in for supplementing usual software (e.g., word processing, spreadsheet, e-mail programme, web browser etc.), may be offered by different vendors. They could provide functionality which may be nevertheless purpose spanning or restricted to one or a few contexts.

Multi-purpose IMA can be realised as a closed system, i.e., it works only in a completed system environment where the managed identities are only relevant or "valid" within the system, such as pseudonyms in eBay.<sup>109</sup> On the other hand open systems work with several independent systems or applications.

Related is the location of storage of identity data: In some systems the data is stored under control of the user, others require a storage and processing on remote servers, especially the service provider. This is a crucial point for the trust model (cf. Chapter 5).

A multi-purpose Identity Management Application could help organising a great part of – but not the entire – technology-based communication.

## 1.4 Actors

For an analysis of an IMS it is important to see who the actors are. As stated before, we concentrate on the relationship individual – organisation<sup>110</sup> (as normal in organisational systems) rather than individual – individual as it would be the case in an interactional system. Thus we assume a digital transaction between the individual, i.e., a user<sup>111</sup>, and an organisation, e.g., an e-Commerce or an e-Government service provider, offering its digital services. Service providers in this context is meant as the direct communication partner of the user. Service providers have to be distinguished from infrastructure providers like telecom operators or Internet Service Providers which only provide the technological basis for the usage of Identity Management Systems by offering the network infrastructure.

Typical scenarios may be an on-line purchase or a request to a governmental authority where the user initiates the connection. It may be as well possible that the service provider initiates the transaction, e.g., in the e-Commerce scenario addressing the user because of his interests or in the e-Government scenario reminding the user to submit his annual tax declaration.

These typical kinds of digital communication are independent from identity management, but its functionality may be integrated into these scenarios. We notice that normally identity management is not an end in itself: It is rather a tool or mechanism to enhance aspects of the communication such as convenience of addressing other parties or being addressed, protection of one's personal data or ease of accessing information about former transactions.

Considering a transaction between a user and a service provider, an IMA installed at the user's side could help the user in handling and managing his identities even without being supported by other parties. This unilateral identity management is restricted in its possible effect, its functionality and accuracy can be enhanced by integration of more co-operating partners (cf. Chapter 2.3.13). The service provider could actively support the user's identity management, e.g., by offering information which might be relevant for the user's choice of identity such as privacy policy or context information.

---

<sup>109</sup> This is at least true unless there is no secondary use of the personal data at the service providers.

<sup>110</sup> The user may be a customer, a citizen or a client, dealing with an external organisation. Or the user may be a member of the organisation itself, e.g., an employee.

<sup>111</sup> In an organisation-IMS, "user" stands for an organisation, e.g., a company or a governmental authority. However, the legal rights and obligations can differ from those of an individual user.

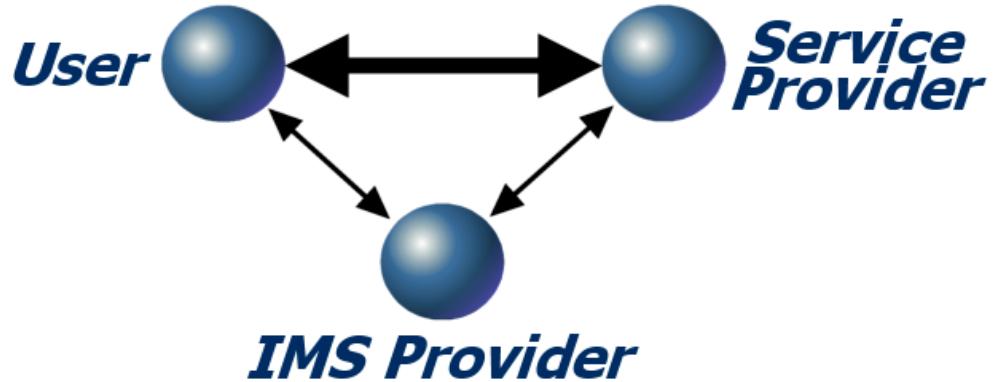


Figure 8: Actors within an IMS – an Abstract Model

If the user is a member of an organisation, e.g., an employee in a company, the constellation can be specified in the following way shown in Figure 9:

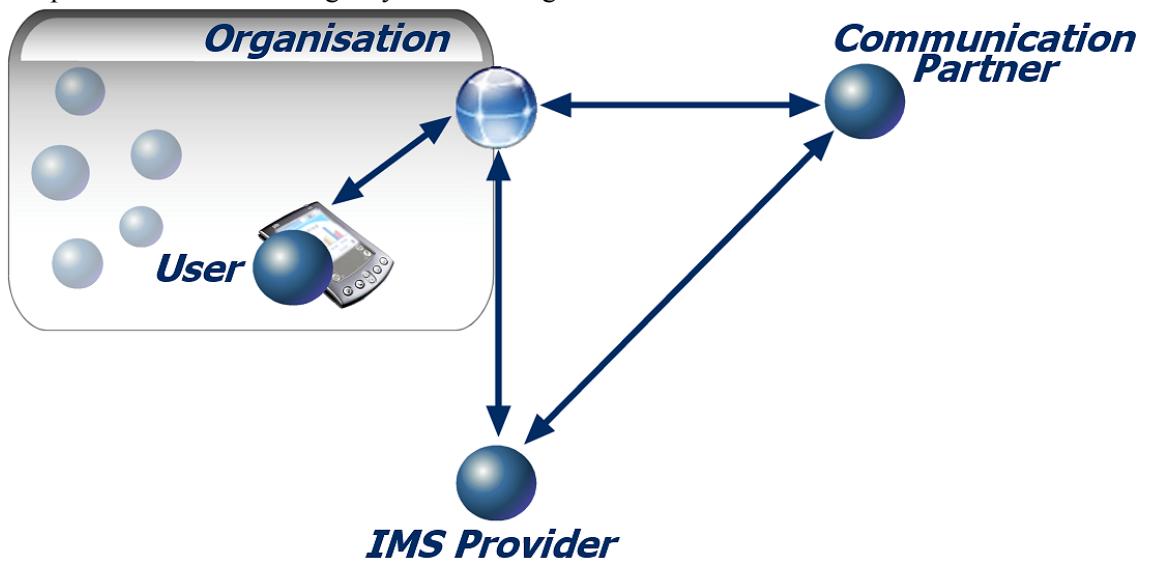
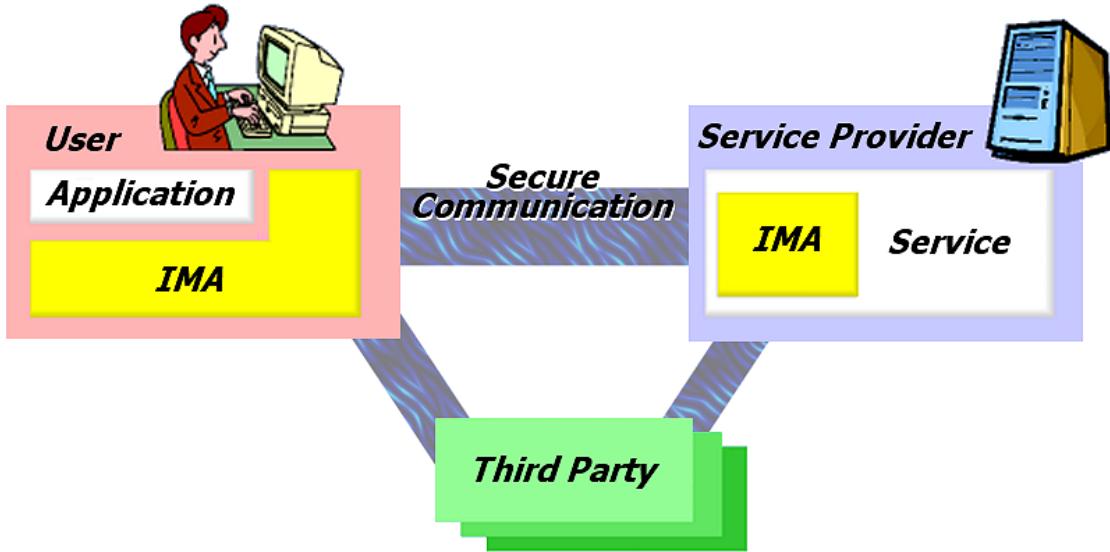


Figure 9: Actors within an IMS – an Abstract Model of an Organisation

Here the organisation may provide the IMA and act as a gateway for all digital communication. This scenario could describe e.g., an employee interacting on behalf of his or her organisation with other communication partners or the collaboration between different teams in various organisations.

The IMS infrastructure needs various third parties. Some of these parties form a PKI (Public Key Infrastructure), providing the certification services needed for secure authentication of users. Trustees may offer different mediator services: *Identity brokers*, e.g., reveal the identity of a pseudonym holder under specific circumstances. *Liability services* clear a debt or settle a claim on behalf of the pseudonym holder. A *value broker* may perform the exchange of goods without revealing additional personal data. *Payment* and *delivery services* can be integrated for a 'separation of knowledge' into (partially) on-line purchases and thereby achieve unlinkability of the 'who (buys)' and the 'what (is bought)'.



**Figure 10: An IMS Model in More Detail**

Further third parties may offer their services, e.g., a privacy information service which may provide information about security and privacy risks and their remedies with respect to the IMA deployed. Of course the user community can help each other as well by exchange of experience, configuration files or software tools.

Moreover, a comprehensive IMS needs a communication infrastructure, which supports basic security and privacy (e.g., network layer authentication, confidentiality, and possibly anonymity) requirements as well as robustness. This infrastructure provided by telecom operators and ISP is the base for all three actors: user, service provider, and IMS provider.

IMS scenarios can determine some roles of users, e.g.:

- E-Commerce: *Consumers* conclude contracts about services and buying and selling things. For example they order books at <http://amazon.com/>, sell things at <http://ebay.com/>, subscribe to mailing lists, ask software-support for help and request information.
- E-Government: A *citizen* is in this context denotes a person who has the nationality of a certain country or state. A person can for example be a citizen of Bavaria, Germany or Europe. There are very different regulations about the way individuals obtain a specific citizenship. It can be associated to the birthplace, the nationality of the father and/or the mother, the duration of living in a country and so on. In order to act as a citizen it is important to know that this status implies special rights and obligations. The latter could be liability to have an ID Card, inform the government of his place of domicile, pay taxes and so on. Rights could be the claim of being protected, voting and privacy protection.
- E-Health: *Patients* have a special interest of protecting their data. Information about the state of health of someone can be interesting for a lot of people to use this data against the patient. The state of health is one of the most intimate facts about a human being. This means special requirements for an Identity Manager in particular for the area of privacy protection.

#### 1.4.1 Users

Users have an interest in some form of IMS when:

- They want to access services for which it is necessary that their qualities or attributes are certified by a third party. Today certain web sites restrict access to credit card holders, even

---

if the service is free of charge. This applies particularly to web sites that require age verification.

- They want anonymity or pseudonymity.

It is common that users do not trust the Internet respectively the security of data transmission. Whenever sensitive data such as credit card numbers, medical information, or application credentials is to be transmitted to an unknown organisation, they will blench from using the Internet. They consider the uncertainty about which data actually will be transmitted and what is going to happen to it as too large [cf. US 2000].

A driving force for identity management therefore lies in increasing need for trust into the Internet respectively e-Commerce. Privacy protection can thereby be laid into the hands of the person the user trusts most: himself. Many people like to individually control what data will be transmitted to whom and for what purpose. This kind of instinctive self-protection includes the desire to be able to validate and understand whatever the identity manager does or has done to gain transparency.

However, a large amount of users prefer a comfortable solution. Their motivation to use an IMA is to gain trust from the use of the identity manager itself. The IMA is intended to automatically care with its preferences for a data processing according to the user's mind and to guarantee a basic standard of protection.

Yet there is not only the wish to control the distribution of one's own personal data, but also to gain certainty regarding the communication partner. Especially for legal transaction it is – from the user's point of view – essential, that both parties can trust into the authenticity of each other. A user wants to know who he is dealing with and to be able to access an easily identifiable real person in case of problems when processing a transaction.

#### **1.4.2 Service Providers**

Organisations have to provide their customers with a certain degree of services related to their identity, not only for billing or law enforcement reasons, but also in order to customise their services.

Service providers' reasons to deploy Identity Management Applications partially coincide with those of the users. Organisations also attach importance to possibilities of increasing data security and influencing the flow of information. Additionally it is often important to them to be clear about the authenticity of the communication partner. Especially cost intensive cases of fraud can hereby be prevented.

The main and most likely only motivation for economically oriented organisations is to increase financial profit. This includes reduction of costs by rationalisation, which is also a source of motivation to non-economic organisations such as governmental organisations. It does include as well data processing to be kept as simple as possible to prevent unnecessary cost. This can be achieved by providing the data to be processed in digital format. To this end, companies can also have an immanent interest in the use of identity managers, this resulting in again more users motivated to use digital technology. They can therewith create trust, possibly resulting in an increased number user visits up to business transactions.

Moreover, there is an interest and to a large extent a legal requirement to keep a company's customer records and other business information accurate, updated and complete. IMA could help hereby to automate the error-prone manual completion of forms etc., as to receive more authentic data.

A related problem of data processing organisations is to design this data processing in compliance to law. Regulations such as privacy protection prescriptions are to be respected by

service providers. IMS can assist organisation in guaranteeing and simplifying this law compliance. By specifically influencing the amount of transmitted data and their quality, data avoidance can be gained in advance and the amount of personal data be reduced, e.g., by use of pseudonyms and credentials.

With governmental organisations, there can be the additional motivation of fulfilling legal obligations, e.g., to use certain technology and to ensure the compliance of additional, even political, requirements.

### **1.4.3     IMS Providers**

Companies providing a certain degree of identification, like Certification Authorities, normally provide some of the services that fall into the definition of an IMS. Such services typically are part of a security chain, required by some kind of on-line business (like server authentication, or SSL encryption, etc.).

The main motivation for IMS providers to use Identity Management Systems respectively to establish the required infrastructure from an economic point of view is the creation of new business concepts. They want to open up new markets that promise lucrative profit opportunities.

Seen from an organisation independent from economic considerations, the motivation for a commitment to establish an infrastructure can instead also be a legal mandate respectively the enforcement of constitutional rights or political aims.

## **1.5     Definition of Related Terms**

### **1.5.1     Definition of Anonymity**

We give both a technological and a legal definition of anonymity.

#### **1.5.1.1     Technological Definition of Anonymity**

To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes. Anonymity is the state of being not identifiable within a set of subjects, the anonymity set [cf. Pfitzmann/Köhntopp 2001; ISO15408 1999]. The anonymity set is the set of all possible subjects.

#### **1.5.1.2     Legal Definition of "Rendering anonymous"**

From the viewpoint of Data Protection Acts the term "anonymising" or "rendering anonymous" is relevant rather than "anonymity". Many Data Protection Acts don't give an absolute, but a relative definition meaning that the effort to a possible re-identification of anonymised, but formerly personal data has to be taken into account: "Rendering anonymous" means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.<sup>112</sup> In the EU Directive Recital 26 it is mentioned that there can be "ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible".

### **1.5.2     Definition of Pseudonymity / Pseudonym**

We give both a technological and a legal definition of pseudonymity.

---

<sup>112</sup> German Federal Data Protection Act Article 3 paragraph 6.

---

### **1.5.2.1        Technological Definition of Pseudonymity**

From the technical point of view, pseudonyms are identifiers of subjects. The subject that may be identified by the pseudonym is the holder of the pseudonym. Pseudonymity is the use of pseudonyms as IDs [Pfitzmann/Köhntopp 2001; ISO15408 1999].

A digital pseudonym is a bit string which is

- Unique as ID and
- Suitable to be used to authenticate the holder and his or her messages.

Using digital pseudonyms, accountability can be realised with pseudonyms [cf. Pfitzmann/Köhntopp 2001].

The concept of pseudonyms is further elaborated in Chapter 2.3.2.

### **1.5.2.2        Legal Definition of "Aliasing"**

From the viewpoint of the few Data Protection Acts which define terms related to pseudonymity, the term "pseudonymising" or "aliasing" is relevant rather than "pseudonymity": "Aliasing" means replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult.<sup>113</sup>

There are already some legal acts which contain the term "pseudonym" in quite different meanings. Therefore the specific properties of the pseudonyms have to be pointed out, e.g., which entity creates the pseudonyms, which entity assigns them to users or personal data, which entities can reveal the identity behind a pseudonym, under which circumstances profiling of pseudonymous data is allowed, etc.

### **1.5.3        Definition of Unlinkability**

As there is no legal definition of unlinkability, yet, we only give a technological definition, taken from [ISO15408 1999]: "[Unlinkability] ensures that a user may make multiple uses of resources or services without others being able to link these uses together. [...] Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system."

We may differentiate between "absolute unlinkability" (as in the given definition; i.e., "no determination of a link between uses") and "relative unlinkability" (i.e., "no change of knowledge about a link between uses"), where "relative unlinkability" could be defined as follows:

"[Relative] Unlinkability of two or more items (e.g., subjects, messages, events, actions, ...) means that within this system, these items are no more and no less related than they are related concerning the a-priori knowledge. This means that the probability of those items being related stays the same before (a-priori knowledge) and after the run within the system (a-posteriori knowledge of the attacker). E.g., two messages are unlinkable if the probability that they are sent by the same sender and/or received by the same recipient is the same as those imposed by the a-priori knowledge." [cf. Pfitzmann/Köhntopp 2001].

---

<sup>113</sup> German Federal Data Protection Act Article 3 paragraph 6a.

## 1.6 Summary

The description of the idea of identity, of identity management and of an Identity Management System in the previous paragraphs illustrates the scope of this study that puts a particular emphasis on the user, their identity and their abilities to control. The further discussion points out the flexibility of modern construction of identity.

The sociological discussion showed the structural differences of social systems (interaction system, organisation system, society sub-system) that vary in their demands on the identity constitution of persons. One decisive conclusion of this study is that particularly in the relationship between persons and organisations, IMS will play an outstanding role. Therefore, the universal IMS must be adjusted to the requirements of particularly this constellation.

The legal discussion, though, was about the historical and legally pragmatic differences between the legal interpretations of identity and identity management. This part of the examination mainly worked out that the conventional positive law of modern states fits Identity Management Systems surprisingly well. The fundamental legal statements, for example, support the basic statements of identity management. But an implementation of the technology-based identity management would require further special laws, though, and the common legal practice would have to be adjusted to the new opportunities.

The technical discussion on the central terms of the technology-based identity management, which has been kept short in this place, was the main aim, which is being tried to achieve with the help of IMS. It is mainly about the management of chains on the basis of addressability through identifiers. Accordingly, it follows that – with an abstract, operation-interested view – real names, too, only serve as identifiers. In this abstract position, it becomes obvious that the use of pseudonyms is sufficient in (socially-structurally or legally) different communicative contexts. Such a use is socially functionally called for and legally covered in most cases. The next technical question is about how to make it as easy as possible for the user to use different pseudonyms for different contexts. A very useful instrument for supporting the user would be something like a "detector of social contexts" that might be made real, e.g., via an Identity Management Protocol [cf. Hansen/Berlich 2003].

Giving a simple overview over the already present IMA and then putting together the set of requirements would be insufficient, because these systems are still at the beginning and there are still no multi-purpose applications. Therefore, this study refers to the considerations in several different disciplines on identity, identity management and Identity Management Systems, and it embeds opinions by experts on IMA and IMS.



## **2 [CHAPTER B: BASIC REQUIREMENTS AND MECHANISMS]**

In this Chapter some general requirements for IMA/IMS are presented as published in literature or in white papers. By analysing several typical scenarios, we then extract more specific requirements, which have to be fulfilled when IMS should be used in these cases. Afterwards mechanisms to meet the requirements are explained and evaluated according their maturity.

### **2.1 Scenarios for Identity Management**

This Chapter sketches various scenarios where identity management is relevant or could be in future. In each scenario firstly the current workflow for handling the concerned task is described. Then the role of identity management is elaborated, giving the benefits and explaining a possible integration – maybe considering necessary modifications in the traditional workflow – of identity management functionality. From each scenario requirements are derived, focusing on the specifics of each scenario where we explicitly concentrate on the demands for the identity management functionality. Additional "common" requirements derived from the application context without a tight relation to identity management will only shortly be mentioned because this would be out of the scope of this study; we give references for further reading.

The scenario requirements, further elaborated in Chapter 2.2, amplify the general requirements for all scenarios where usable and reliable ICT are involved. We choose typical scenarios from different social contexts. Each of them is relevant to a big population group. Similarities and some main structural elements will be analysed in Chapter 2.1.7.

However, it should be noted that all scenarios only describe a small sector of the whole world. Each of them has interfaces to other scenarios, and in all cases there are situations before and after (pre- and post-processing phases) which are not elaborated in this Chapter. Most interesting would be an arbitrary combination of scenarios, representing a real multi-purpose (or all-purpose?) use of and in IMS. This visionary part will be discussed in Chapter 7.2.

#### **2.1.1 General Identity-Related Scenarios**

Before pointing out where IMS can be integrated, we illustrate two general cases with respect to identity:

- Identity Theft, which is related to insufficient authenticity, and
- Data Trails, which are related to insufficient anonymity and transparency.

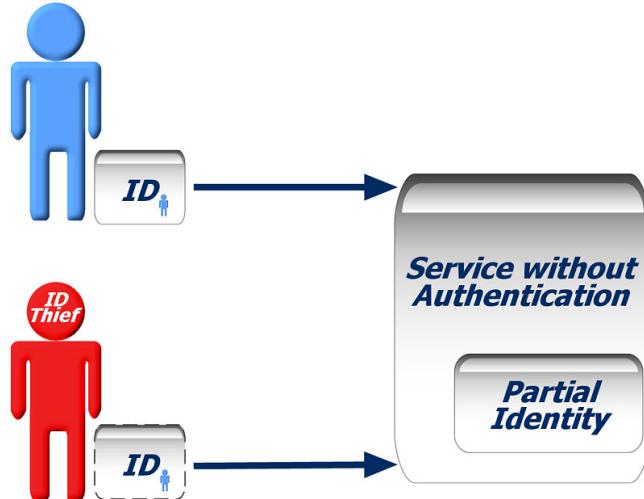
Detailed scenarios focusing specifically on authentication or on anonymity are outside the scope of the study, but we give some ideas on the general problems in today's digital networks.

The main security aspects of confidentiality, integrity and so on are always processed. Identity management bases on security surely, but the characteristic problems of identity management are mainly independent of this and are focused on a new type of problems.

##### **2.1.1.1 Identity Theft**

Although identity theft is not a problem which is restricted to the digital world, it has become a serious problem in the last years, especially in the US [cf. LIBE 2003]. Identity theft describes the attack of capturing of identity data of another individual in order to profit from the victim's reputation or authorisation or to damage the victim's reputation. It is possible whenever there is no strong and secure authentication method.

When no authentication is required, it is easy to capture an identity, e.g., sending e-mails under the name of another person or filling in credit card numbers of other people which may or may not be known by the attacker.

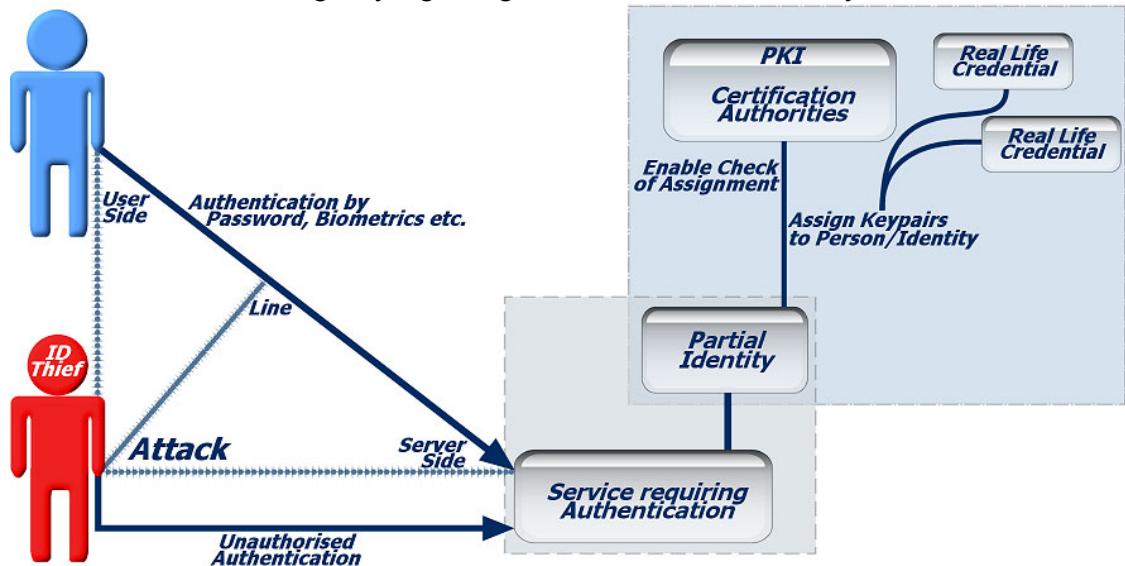


**Figure 11: Identity Thief Using Services without Authentication**

In some cases the identity thief is not been able to capture back channel, especially when authentication is necessary, e.g., the attacker could send e-mails under another person's name, but won't receive the replies.

Stronger and more secure authentication methods help in coping with the identity theft problems:

1. Direct authentication before using service;
2. Authentication of messages by digital signatures; certificates issued by a CA in a PKI.



**Figure 12: Attack Points of an Identity Thief in a Scenario with Authentication**

Still identity theft may be possible. Figure 12 illustrates possible points of attacks:

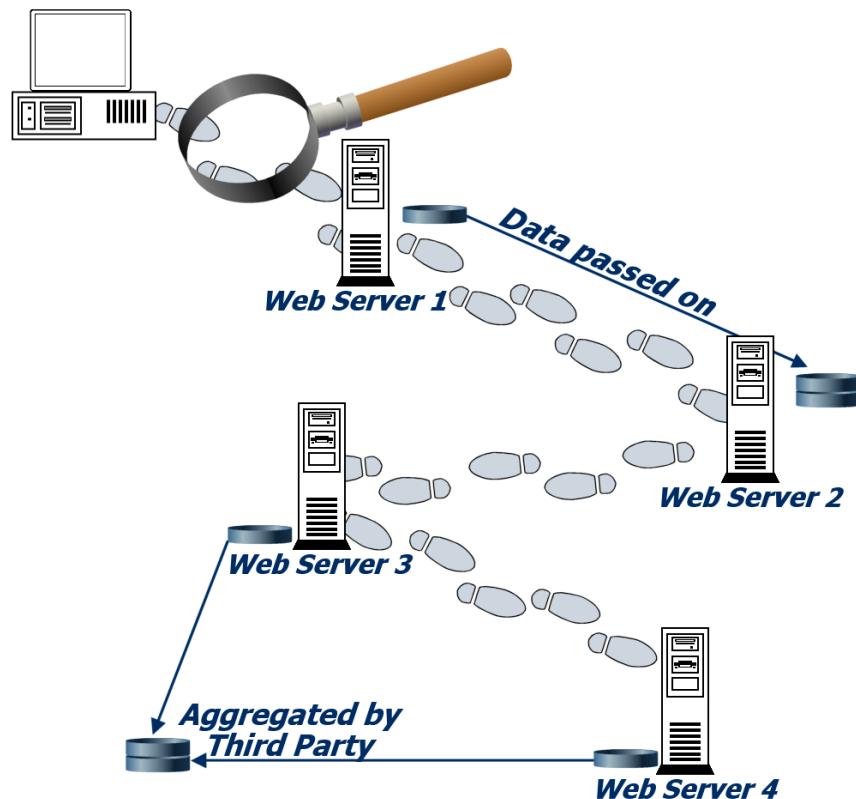
- User side (trojan horses, key loggers),
- Server side (security breach, hacking database with references of authentication data) or
- Line (tapping, sniffers, man-in-the-middle attack).

If such an attack is successful, the full digital identity in this context can be captured, mostly including the back channel. Because of methods of stronger authentication it is more difficult for the victim to prove that it is not he or she who is acting.

### 2.1.1.2 Data Trails

Today's Internet use means leaving data trails which goes unnoticed by most users. Examples are shown in Figure 13:

- Web servers log IP addresses of the user.
- According to the protocol HTTP, a web server passes on referrer information when the user follows a link to another web site.
- Third party cookies even enable the aggregation of various usages over a longer period of time.



**Figure 13: Data Trails When Using Internet Services**

In fact the user has no real control over when which data is disclosed and who may derive what knowledge from this information.

Figure 14 illustrates which parties are integrated in a normal Internet access and what logs are typically taken [cf. Köhntopp/Köhntopp 2000]:

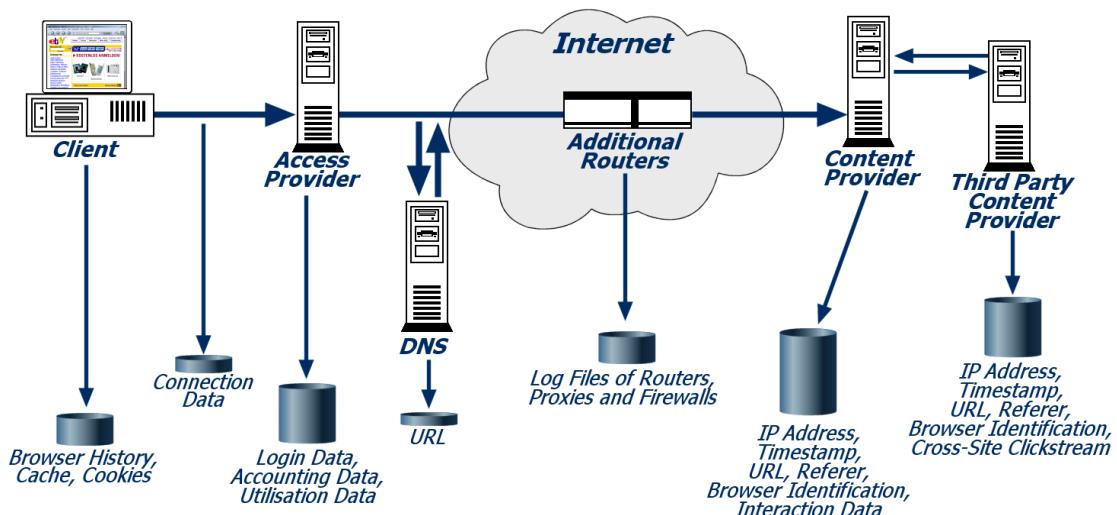


Figure 14: Typical Logs at Different Parties

## 2.1.2 General Scenarios

After having recognised two main problems, we begin with three general scenarios, which prepare the ground for more specific ones.

### 2.1.2.1 The IMA as a Gateway to the World

#### Description

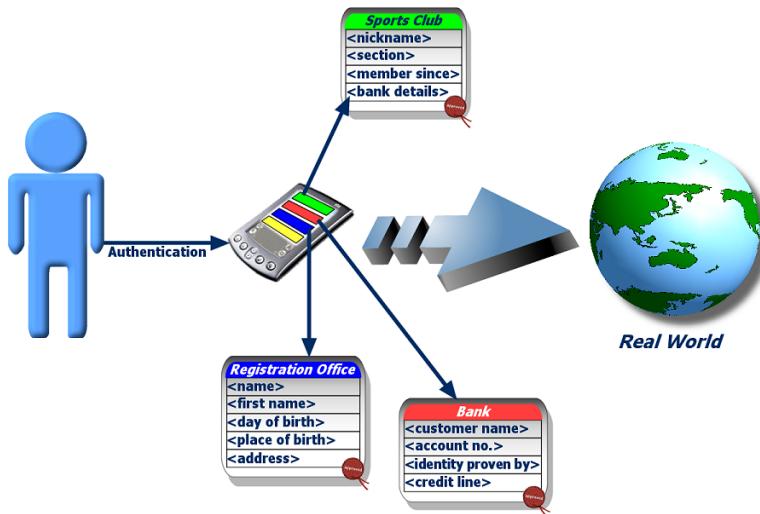
To envision what a multi-purpose IMS could look like, we have to imagine various use cases. In general the IMA should help in managing identities, meaning that different pseudonyms with associated data sets can be used according to different roles the user is acting in and according to different communication partners. Those pseudonymous data sets could be certified as being issued by organisations like a registration office, a bank or an association (external authentication), or they could be generated by the user himself/herself (self-authentication). An important technology for detecting interaction contexts will presumably be an Identity Management Protocol Set (cf. Chapter 1.3.1).

In the sequel we speak of *Pseudonym Domains (PD)*<sup>114</sup> in which a subject is known under a unique identifier or pseudonym. Each Pseudonym Domain defines the scope of the pseudonym; outside it may not be relevant anymore. For each Pseudonym Domain the properties, the pseudonym must have, can be different. The user himself/herself or third party entities, which are in multiple Pseudonym Domains may perform the task of creating new pseudonyms and assigning them.

The IMA would be the gateway and guardian in digital communication with the world, comprising all scenarios in which the user would like to manage his or her identities. It could be realised within a device on its own, possibly having additional functionality, e.g., like a PDA or a mobile phone with address books and the possibility to establish connections to one or more networks. It could also be a plug-in or another additional software, e.g., a proxy, enhancing the Internet access by browsers or e-mail clients, being today responsible for a lot of digital communication. If the IMA is implemented as a proxy, it may run locally on the user's PC, or an

<sup>114</sup> Pseudonym Domains are similar to "pseudo-identity domains", which have been introduced earlier by John Borking when proposing the concept of the identity protector: "To implement matters technically, a system element called the 'identity protector' is used within the data system to convert the identity of the person involved (the person whose data are being processed - the 'data subject') into one or more pseudo-identities. The placement of the identity protector provides for at least two different domains within the data system; one domain where the identity of the person involved is known or accessible (the identity domain) and at least one domain where this is not the case (the pseudo-identity domain). The aim of the pseudo-identity domain is to make sure the person involved cannot be traced on the basis of previously obtained personal data, and vice-versa, to make sure the personal data cannot be found on the basis of the obtained identity." [cf. Borking/Raab 2001]

IMS provider may provide it remotely. Specific identity management functionality may even be implemented in an operation system and in all OSI network layers – but today these are mere visions of the future.



**Figure 15: IMA as a Gateway to the World**

### Motivation for IMS

As already described in Chapter 1, there are different possible motivations and drivers for identity management, e.g.

- Convenience for managing existing identities and addresses, e.g., different usernames;
- Authentication and access control, e.g., single sign-on services or digital signatures;
- Role management, e.g., separating the professional and the private life;
- Reachability management, e.g., determining who may call or address oneself in which situation, e.g., limiting spam;
- Right to informational self-determination, i.e., balancing anonymity and authenticity, and expressing and enforcing the user's privacy preferences;
- Stake holder interests in managing data on behalf of a user or profiting from new business models, especially in third party services.

The policies of such services and systems are shaped differently, depending on their aim or motivation. The users, the service providers or the IMS providers, can be the driving force behind such services.

The separate Pseudonym Domains are defined by use of each of the pseudonyms with associated data sets. In this general IMA scenario, the user is the main entity to manage pseudonyms, but also third parties providing certificates or other person-related data (including pseudonyms) can create pseudonyms and/or assign them to a user if this is required or desired.

### Requirements

The following requirements apply to the general scenario and form the standard demands to IMS, which may be extended in specific contexts and scenarios. The categories have been chosen according to [ANEC 2003].

**Table 1: Requirements in the General IMS Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	The specific functionality for each scenario has to be fulfilled like identity administration, gateway, notice and control
Usability	Basic usability for all participants in the system, being implemented in system design, documentation, and possibly support, is a mandatory requirement.
Security	For security relevant intentions a mutual authentication could be important. Availability of the services is important to foster trust among the users. The same applies for integrity of data. A non-reliable service will not be used. Confidentiality breaches are not as easily noticed as failures of the system availability. As far as sensitive data are concerned, confidentiality measures should be taken.
Privacy	The support of the individual's right to informational self-determination and to privacy is necessary to really enable the user to manage the identities, i.e., personal data. Of course the legal requirements, which can differ in the various scenarios, have to be fulfilled.
Law Enforcement	The legal requirements, which can differ in the various scenarios, have to be fulfilled. In some cases there may be no need for extra law enforcement requirements, e.g., because the IMS is used in legally non-relevant communications or because a misuse cannot happen. Generally speaking for providing fair exchange <sup>115</sup> either there has to be a performance bond of the contract or there should be enough significant digital evidence to prove one's position in court.
Trustworthiness	Measures for objective trustworthiness of the IMS (by implementing usability, security, privacy and law enforcement functionality where appropriate) should be taken, supported by measures for gaining trust.
Affordability	The integration of identity management functionality should not make transactions far more expensive than the actual one. If possible, by integration of this functionality the participants also strive for additional economical advantage by creating new business models and services.
Interoperability	The new functionality should be both compliant to legacy systems and to new standards.

As the categories "Trustworthiness" and "Interoperability" are not applicable in specific scenarios rather than in this general notion or in specific products, the following scenario requirements leave out their description.

### 2.1.2.2 Identity Protector

The Identity Protector is a concept for integrating privacy functionality into information systems [cf. van Rossum/Gardeniers/Borking et al. 1995]. Conventional information systems perform the following five transaction phases: authorisation, identification and authentication, access control, auditing, and accounting. At each phase, a user's identification is connected with the transaction. The Identity Protector introduced into an organisation's information system would control the exchange of the user's identity within the system by splitting it into different "pseudo identity domains" and tailoring the information disclosed according to those domains (cf. Figure 16).

<sup>115</sup> Fair exchange assumes a prior agreement among the parties before proceeding to the exchange. A fair exchange is achieved if two conditions are met: atomicity and fairness. Atomicity means that all agreed transfers of information are performed, or none are performed. Fairness means that the parties actually receive what they agreed to receive. Fairness requires that the parties specify what they expect from the exchange. Upon receipt, each party verifies that what they received matches their specified expectation. Fair exchange is often realised by support of third parties. Protocols have been proposed to minimise the trust in additional third parties [Lacoste/Pfitzmann/Steiner/Waidner 2000].

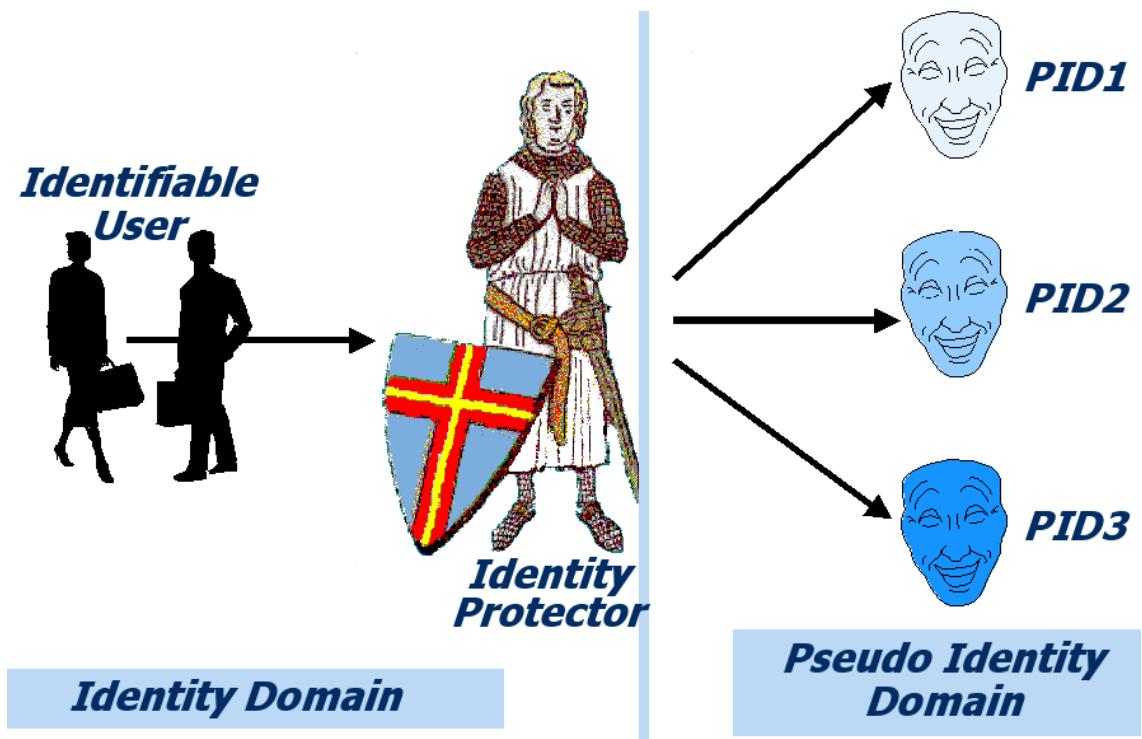


Figure 16: Identity Protector and Different Pseudo Identity Domains

The information system would have to be structured in a way as to remove all unnecessary linkages to the user's personally identifying information. From this notion, an IMS can be regarded as an Identity Protector, which is directly controlled by the user. However, normally the concept applies to information systems themselves and their managing of personal data rather than integrating the user as an active participant for managing personal data and asserting his or her rights to privacy. The Identity Protector could act as guardian between different pseudo identity domains (cf. Figure 17).

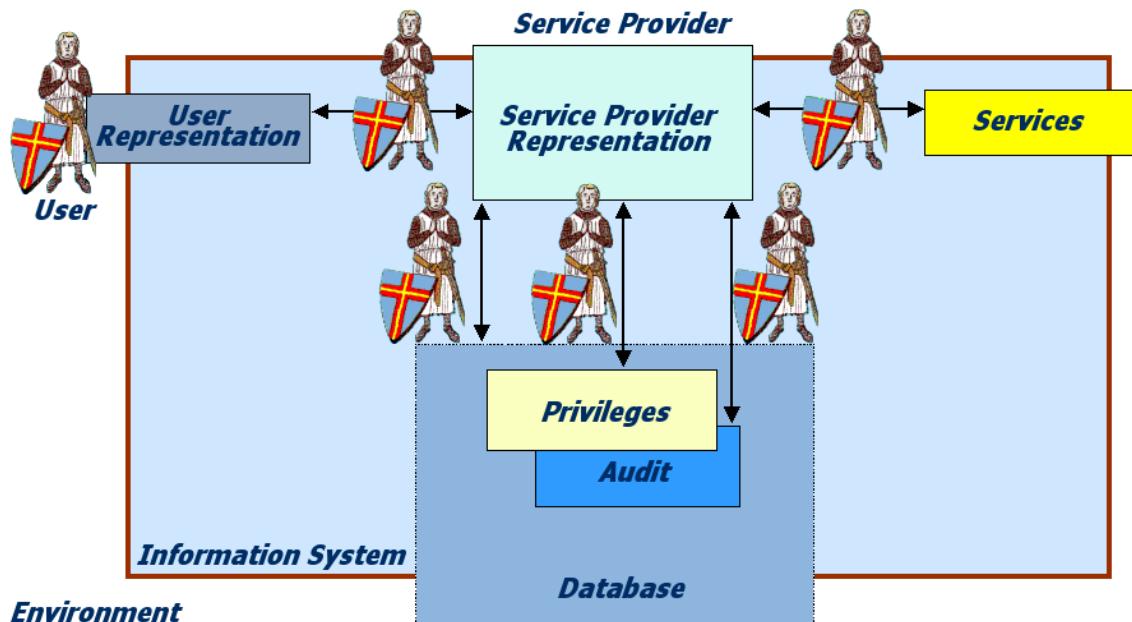


Figure 17: The Identity Protector in an Information System

By now, some application-specific Identity Protectors have been built, but in most cases not directly controlled by the user, or at least not in their own sphere of control.

### 2.1.2.3 Task Assignment Scenario

Also in the IMS context, the system design has to be taken into account, being able to support the use of pseudonyms or to anonymise or pseudonymise actively within the organisation. One basic scenario is the ordinary process of assigning tasks in an organisation without giving the staff the real name of the requesting person. While at first glance this seems to be a sophisticated undertaking, it is quite common not to give the real name to the staff if, e.g., a medical lab performs an examination by order of a doctor or if an academic text is passed to reviewers for being evaluated. This internal pseudonymisation in an organisation does not only realise privacy and security principles like restricting the information to what is necessary ("need-to-know principle"), but also aims for a fair and equal treatment of requesting persons without reservation or risk of privileges or discrimination.

#### Description

Figure 18 shows the workflow of a client, requesting something from an organisation (e.g., a sales company or a local authority). The organisation employs several staff persons (officials or clerks) in charge to whom those requests could be assigned by the organisation office according to a certain distribution key. The first contact of the client is made under an address to which the response will be sent later on. Pseudonym Domain 1 comprises the client and the main office of the organisation that both know how to address the client for answering his or her request. For performing the given task, the job is forwarded to a staff person who does not necessarily get to know the same identifier of the client, but may work with a second pseudonym. Today in this second Pseudonym Domain internal reference numbers are often used rather than the real name. After having carried out the task, the staff person reports the result to the office which may take further steps and send a response to the client.

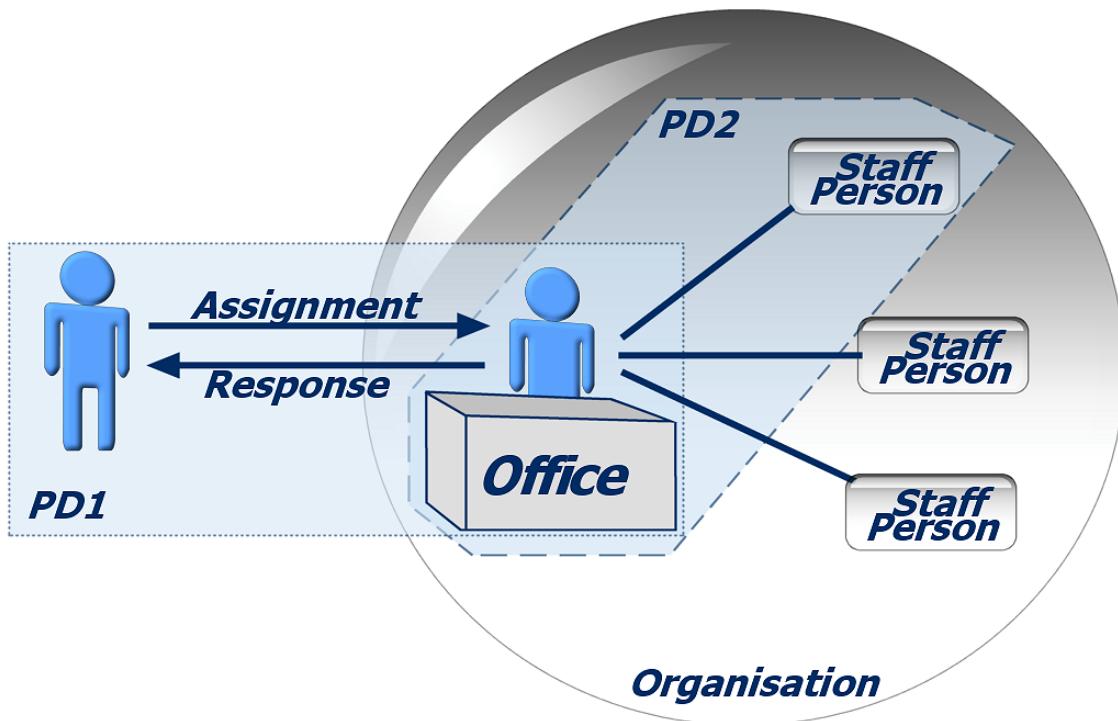


Figure 18: Pseudonym Domains in Assignment of Tasks

#### Motivation for IMS

Both the organisation as well as the client can be interested in the carrying out of the order without respect of the person. For the purposes of a "righteous world", this could be even socially called for. The organisation office serves the distribution of the tasks and the separation (a kind of "de-linking" or "de-coupling") of the relationship between the client and the staff

person as well. Dealing in content with the client or the order is not the subject of the office and its employees.

Pseudonym Domain 1 exists between the client and the organisation office. If it is an order relationship that is based on the possibility of a repetition, both parties may be interested in the possibility to use the same pseudonym more than once, e.g., for building up a certain reputation, for reconsiderations and checks or for offering client-related benefits. If this is not desired, the client can use a new pseudonym for each order. This pseudonym is only valid and can be addressed by the organisation until the order has been finished.

Pseudonym Domain 2 comprises the organisation office and its employees. In order to guarantee the independence of the person in charge's judgement, this pseudonym can be decoupled from Pseudonym Domain 1. The people in charge are then not able to access any client data other than those transferred.

Of course the translation between both pseudonyms has to work properly so that the result elaborated by the staff person really reaches the requesting person. The office as both separating and linking instance is very important in this scenario, acting as an Identity Protector. The internal use of a pseudonym (as of a reference number) is not necessarily known nor can be influenced by the client.

In some cases the idea of anonymising the request renders useless, e.g., when personal data is directly bound to the request and cannot be stripped off without losing information.

### **Requirements**

**Table 2: Requirements of the Processing of Orders Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Reliable re-pseudonymisation of organisation office; Pseudonym I: durable for processing of order until conclusion, addressable by organisation, re-use possible for special advantages Pseudonym II: durable for processing of order until conclusion
Usability	Easy to use, belongs to order
Security	Important
Privacy	Prevention of profiling by organisation
Law Enforcement	Possibly requirement of linkability in the organisation office
Affordability	Depends on order

### **2.1.3 E-Commerce**

#### **2.1.3.1 E-Shopping**

##### **Description**

The main actors in this scenario (cf. Figure 19) are the customer and the seller (e.g., in an Internet shop). The customer visits the site of the seller and inspects the offerings. When he has questions about a product or needs advice what to buy, he asks the seller using e-mail, fax or telephone. The seller answers the request using the same medium.

After the customer has decided to purchase something in the Internet shop, he places an order. For this he can use the shop system, e-mail, fax, telephone, mail etc. Usually, this order contains not only the declaration about the good to buy, but also the name of the customer and address information. In order to accelerate processing it is possible that he tells the seller also his credit card number or bank address.

---

It could also be desired to provide special sub-attributes like, e.g., vouchers, trading stamps or customer ID for special discounts; the seller may also ask for an age verification etc. in particular situations.

Both the seller and the buyer are interested in the other party fulfilling their obligations, i.e., that the seller sends the ordered goods and the buyer pays the price as agreed. If there were business connections before, the gained reputation influences the current transaction. The latter is also influenced by a professional and respectable appearance or other peoples' experiences. If the seller does not trust in the buyer's solvency or payment pattern, they can ask for an advance payment or the buyer's bank account data for a direct debiting. On the other hand, the buyer can ask for an advance delivery of the products.

Either the buyer asks his bank to transfer the purchase price to the seller's account. Or he uses his credit card. If he uses his credit card, he gives his credit card number, the valid date and name to the seller (1). The seller asks the credit card company to remit the money (2) and the company will do so if the data check yields positive results (3). Normally at the end of a month the credit card company charges the customer (4), and the customer transfers the money to the credit card company (5) or grants the permit to debit it directly from his bank account.

In return for the bank transfer or the usage of the credit card, the seller ships the goods. With digital products, this can be achieved directly, e.g., by enabling a download. With respect to non-digital products, there is a need of physical delivery by a transport company (e.g., post, UPS etc.).

The delivery finally takes place at the buyer's place or at a pickup point (e.g., poste restante, neighbours, gas station etc.) where the buyer picks up the goods after identity verification.

The currently most popular way of ordering or buying products is the enabling of the shipment by giving the customer's name and address. The payment transfer takes place with giving the customer's name and bank account data to make sure the seller can directly assign the payment to the payments agreement.

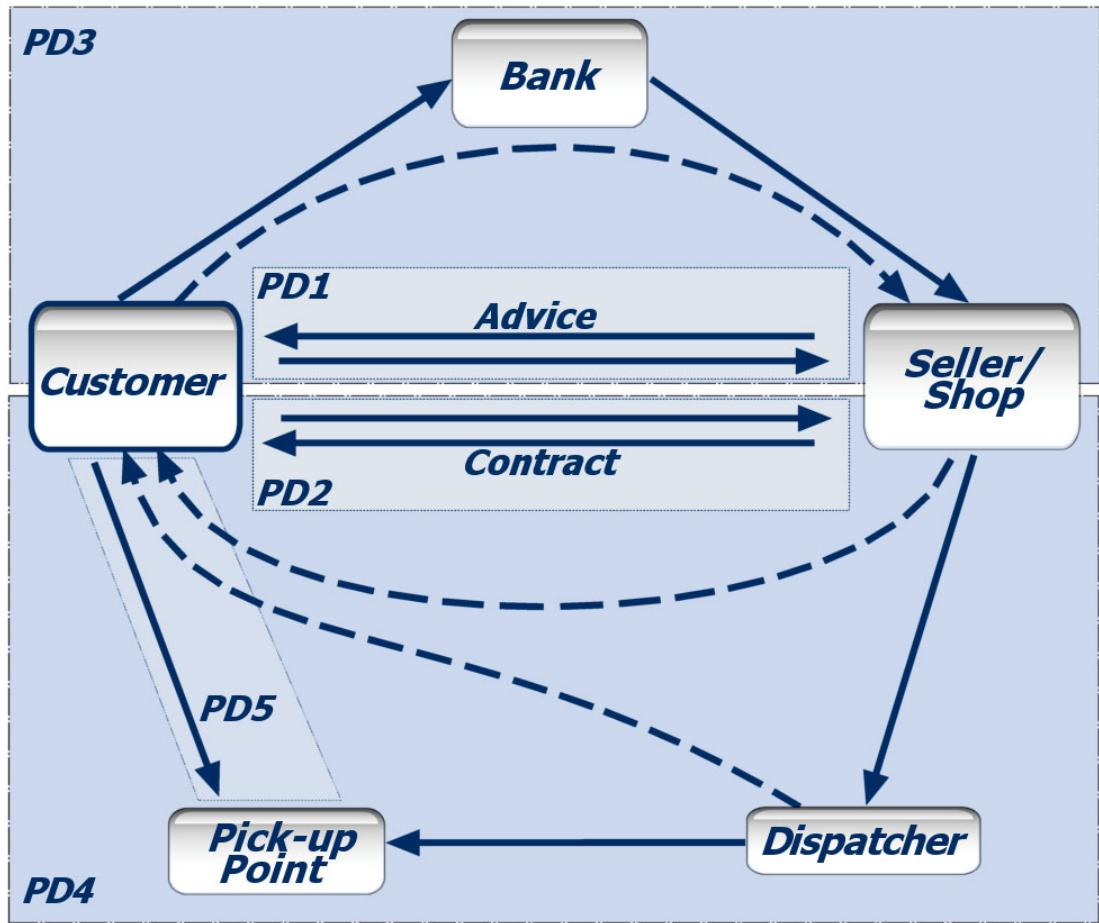


Figure 19: Pseudonym Domains of a Customer in an E-Shopping Scenario

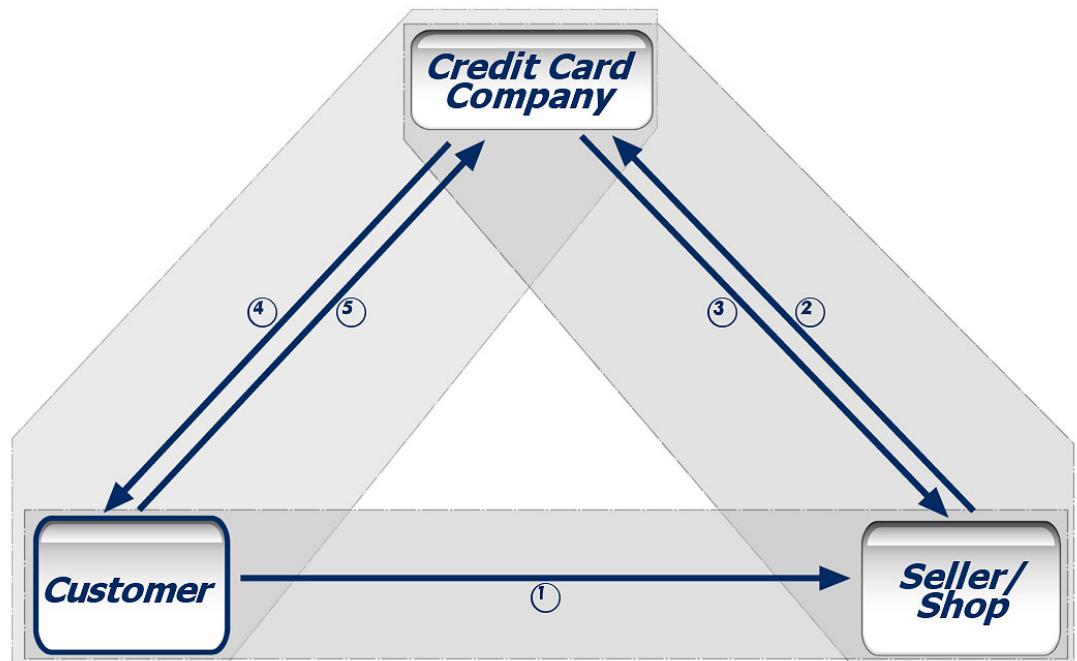


Figure 20: E-Shopping Scenario and Paying with a Credit Card

---

## **Motivation for IMS**

The IMS can be deployed for the guarantee of the buyer's anonymity. This can be desired to avoid the establishment of a profile and therefore linkability with the purchase of sensitive products, or to enable an independent consultation, or to prevent an undesired mailing of promotional material.

In order to achieve this, the customer can act under different pseudonyms (cf. Figure 19). The customer may already use a pseudonym in the consultation phase, which cannot be traced back to them (Pseudonym Domain 1). For the actual purchase, a different pseudonym can be used that cannot be related to the consultation pseudonym (Pseudonym Domain 2). This one can be linked to a certain reputation to ensure the seller that the payment will be made. Alternatively, a special, individual pseudonym might be assigned to each seller which can be used every time the buyer gets in contact with the seller to whom it is assigned, in order to build up the reputation of a regular customer and at the same time to avoid a linkage of the customer's data with those at other sellers.

It is not absolutely necessary to use a personal pseudonym or process customer data for demands on warranty service. It would rather be sufficient if the customer would exhibit the digitally created bill or invoice for which personal data are irrelevant. The customer could even use such bills and invoices for their tax declaration. For recalls, e.g., for security reasons, a provision of addressable pseudonyms could be useful. However, in many cases, customer data are not being stored nowadays, therefore recalls are being carried out via broadcast announcements. This could be carried on.

Furthermore, the deployment of credentials for different sellers or sales departments within a company could be useful if a certain reputation is to be included but the creation of a profile is to be avoided. Such a reputation could be confirmed by a trust-worthy third party that guarantees the payment for the purchase up to a certain sum, like, e.g., a bank. Such a third party which both seller and buyer trust could even be directly involved in the payment procedure as a value broker to care for the synchronous exchange of money and products.

The shipment, too, can take place by using a pseudonym. It would be possible to use a pseudonym given by the customer which the seller cannot assign to personal data but which the company can assign to an address (e.g., iprivity.com) (Pseudonym Domain 4). Another possibility could be to ship the products to a pickup point where the buyer can collect them after identity verification (password, PIN etc.). Both variants do not necessarily imply a personal identification in the view of the seller or can take place by use of a special pseudonym.

The Pseudonym Domain 3 includes the payment procedure, which is a part of the e-payment scenario and will be detailed there (cf. Chapter 2.1.3.3).

## **Requirements**

**Table 3: Requirements of the E-Shopping Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Pseudonym I: durable for the advice until finishing, addressable by the seller / adviser; Pseudonym II: long durability, re-use possible to establish reputation; Addressability of pseudonym if customer wants to get further messages from seller; Pseudonym III: for money transfer (cf. Chapter 2.1.3.3); Pseudonym IV: durable for the shipment, addressable by the dispatcher
Usability	Easy to use because of usage by every normal customer
Security	Important (cf. general scenarios), esp. prevention of identity theft and misuse of, e.g., credit card numbers; non-repudiation of the user; prevention of accidentally false addressing
Privacy	Prevention of profiling, anonymity of the customer;

	At the user's side: logging of legal acts, storage of contracts / general terms and conditions
Law Enforcement	Digital evidence necessary in case of identity theft, reputation theft, warranty (e.g., receipt), wrong delivery ...
Affordability	Cheap, for every-day use and every-person use

### 2.1.3.2 E-Auction

#### Description

Actors in this scenario are the seller, the auctioneer, and the customer who later on turns out to be the highest bidder and therefore will buy the good.<sup>116</sup>

The seller places his good in the e-auction system of the auctioneer (using his pseudonym which could have a special reputation). The buyer bids for the good and gets the acceptance if he is the one with the highest bid at the end of the auction time. The auctioneer sends both, the seller and the buyer, an acceptance mail with the personal information of the other one. Customer and seller discuss the way to exchange money and good.

Then normally the buyer transfers the money to the seller and after arrival of the money the seller send the good with a dispatcher to the buyer. Another typical way is to send the good instantly to the buyer and let the dispatcher collect the money before handing over.

Some auction systems – especially when offers and bids are made by use of pseudonyms – include an evaluation mechanism between seller and buyer to build up a reputation that can be viewed by all other participants.

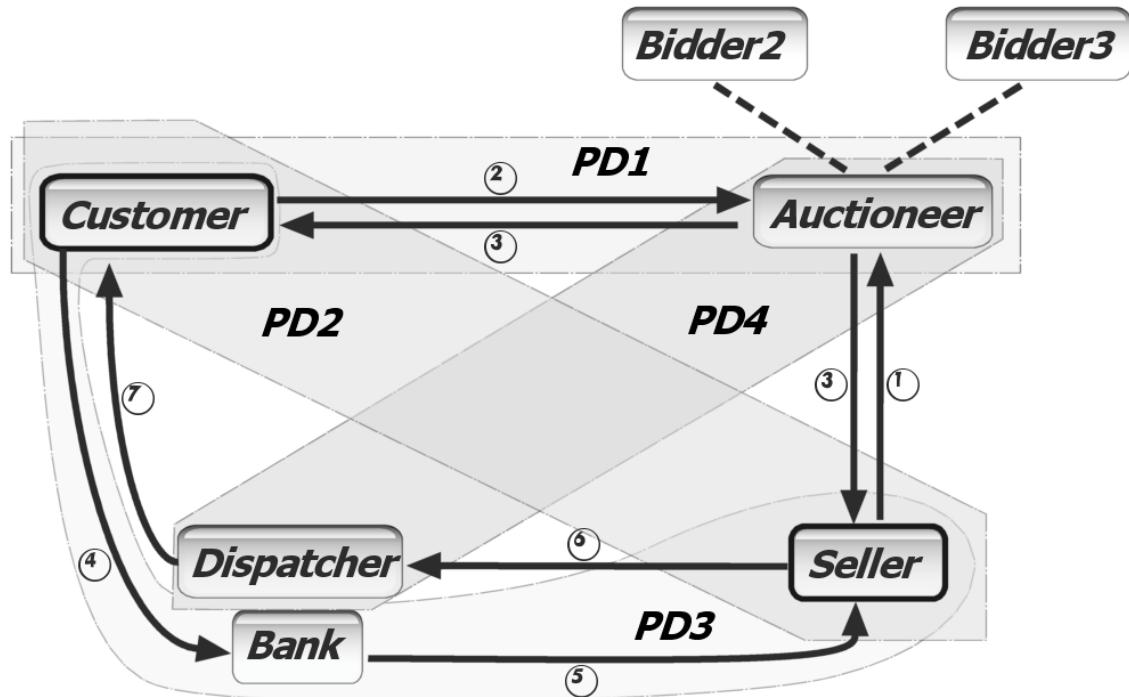


Figure 21: Pseudonym Domains of Customer and Seller in an E-Auction Scenario

#### Motivation for IMS

Both the bidder and the seller could be interested in remaining anonymous towards each other. This is intended to avoid the building-up of profiles; nobody shall get to know what someone buys or sells, and undesired profiling, e.g., for targeted distribution of promotional material, is

<sup>116</sup> There are various ways of settling auctions. In some auction systems, also, e.g., the second highest bidder is paid attention to. In this place we refer to the pattern used by eBay.

---

to be prevented. At the same time, building up a reputation for one's own pseudonym is desired. It might be conceivable to deploy different pseudonyms with reputations / attributes for different purchases / item groups.

Reputation systems are defined as follows:

"A reputation system gives people information about others' past performance. It can enhance an on-line interaction environment by:

- Helping people decide who to trust;
- Encouraging people to be more trustworthy;
- Discouraging those who are not trustworthy from participating."<sup>117</sup>

In general it is a challenge to combine IMS and reputation systems because reputation means linkability of actions whereas anonymous behaviour cannot get high reputation scores [cf. Resnick/Zeckhauser/Friedman/Kuwabara 2000; Kreps/Wilson 1982; Tadelis 1999; Cranor/Resnick 2000; Friedman/Resnick 2001].

Figure 21 shows the different Pseudonym Domains: Pseudonym Domain 1 describes the relationship between the bidder and the auctioneer. By use of credentials or different pseudonyms, the auctioneer and possible observing third parties are prevented from building up a profile of the bidder. The duration of the pseudonym is limited to the moment when a higher bid is made.

Pseudonym Domain 2 describes the relationship between the bidder and the seller. The seller is to know the reputation of the bidder (buyer) but otherwise the latter should remain anonymous. The auctioneer, too, is to be prevented from the possibility to build up a profile of the bidder and a linkage to other purchases. However, the pseudonym has to be addressable as far as the seller must be able to assign the products to the buyer and make an evaluation to influence the buyer's reputation.

Pseudonym Domain 4 describes the relationship between the auctioneer and the seller. In order to prevent the seller from building up a profile of the buyer, the auctioneer (or the buyer) could communicate only a one-time pseudonym for the shipping, which is mentioned on the products to be shipped. The assignment of this shipment pseudonym then takes place at the transport company. The duration of this pseudonym is limited to the time of transportation until the arrival at the buyer.

The payment for the products can again take place by use of a special pseudonym (Pseudonym Domain 3) (cf. Chapter 2.1.3.3).

### **Requirements**

**Table 4: Requirements of the E-Auction Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Pseudonym I: durable for the bidding process until finishing or overbidding, addressable by the auctioneer; Pseudonym II: long durability, re-use possible to establish reputation; Pseudonym III: for money transfer (cf. Chapter 2.1.3.3); Pseudonym IV: durable for the shipment, addressable by the dispatcher
Usability	Easy to use because of usage by every normal customer
Security	Important, esp. prevention of reputation theft, identity theft and manipulation; non-repudiation
Privacy	Prevention of profiling, anonymity of the customer/bidder; At the user's side: logging of legal acts, storage of contracts/general terms and conditions

---

<sup>117</sup> Paul Resnick; <http://si.umich.edu/~presnick/>. See also <http://databases.si.umich.edu/reputations/>.

Law Enforcement	Digital evidence necessary in case of identity theft, reputation theft, warranty, wrong delivery, fulfilment ...
Affordability	Cheap, for every-day use and every-person use

### 2.1.3.3 E-Banking

#### Description

The function of a house bank – and particularly a house bank as the main financial institution – is to manage the customer's money and carry out financial transactions as ordered. The customer draws on his or her account, transfers money to another account or deposits it. This can take place with other currencies and in various forms (cash, checks, micropayments, digital money, cash card, M-Pay, PayBox etc.). In addition, the house bank manages and arranges credits, insurances, and securities of the trading systems; in some cases special credit cards are handed out.<sup>118</sup> When opening an account, the bank has to verify the customer's identity.<sup>119</sup> The banker's secrecy plays an important role since all information comes together at the house bank.

The establishment of home banking diminishes this function of the house bank as a central arrangement authority in an increasing manner: A house bank still connects its customers to the financial sphere but, however, an increasing number of customers get in sovereign touch with banks with the specialised business areas and settles these transactions (mortgages, credits, leasing, shares, pensions insurances) directly. The house bank becomes one instance among others. National borders no longer limit even bank transactions of private customers.<sup>120</sup>

As far as the increasing number of the electronic ways of payment is concerned, the meaning of the house bank changes in still another way: Just like the traditional cash, money in its digitised form can also be exchanged directly between the people involved ("peer-to-peer payment"). In this sense, the banks do not necessarily have to carry out transfers as an arrangement instance but will (now and then) be used as a clearing instance that issues, confirms and redeems the digital form of the money or pass it to the customer's account.<sup>121</sup>

Another property of traditional cash in the form of coins and banknotes is that transactions can take place anonymously, i.e., without a data exchange between the persons involved and also without a reference to an object. This property is not only privacy-sympathetic but also generally functional under the aspect that the history developed until the decision to pay can be erased or dies with the payment. Therefore, also the digital forms of payment have to include this socially very functional property of the forgetting of the history – or, to express it in the technological way, of the unlinkability of events. Indeed it seems as if the tendency rather moves in the direction of linking every transaction of digital money to a bank (more on digital money cf. [Schneier 1996] and [Lacoste/Pfitzmann/Steiner/Waidner 2000]).

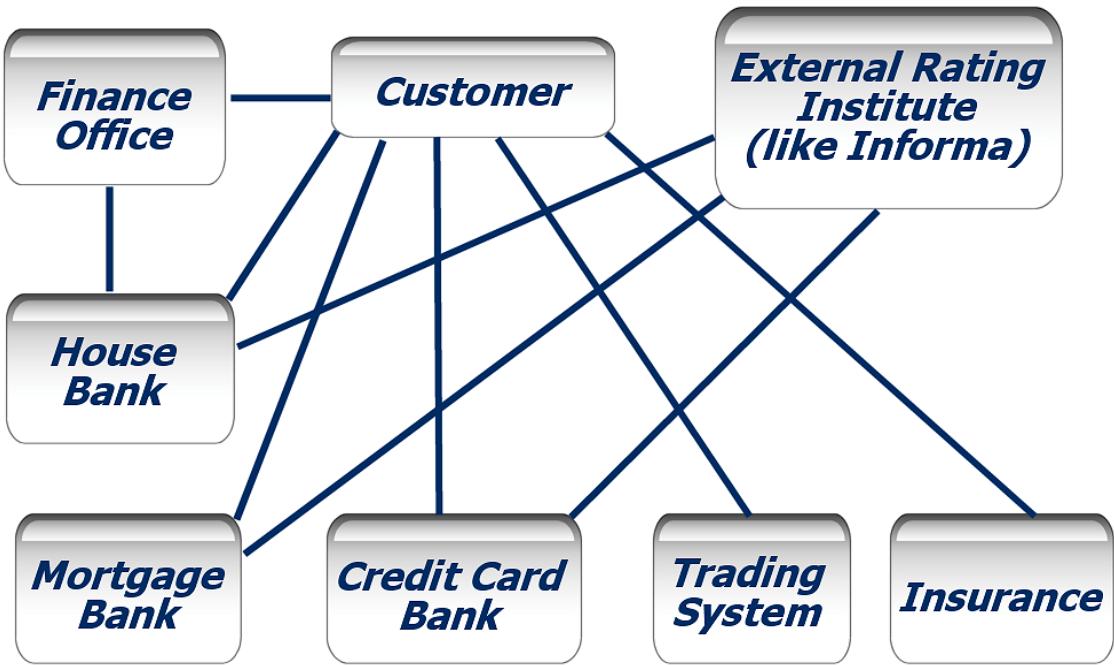
---

<sup>118</sup> Especially in Germany, banks have to pay those taxes that are related to the security trade directly to the Treasury and identify and document transfers that exceed sums of 15,000 EUR, according to the German Act on tracking down Profit from serious criminal acts (25.10.1993, last modification 15.08.2002). Cases of suspicion of money laundering or financing of a terrorist group must be reported to the central office for suspicion reports of the Federal Bureau of Criminal Investigation.

<sup>119</sup> This applies to numbered accounts in Switzerland (according to the principle "know your customer"). The group of people who could be able to refer an account number to the identity of a customer is kept very small, though. It is well known that the banker's secrecy (according to which the account data belong to the customer and not to the bank) is the ultimate fundament of this business.

<sup>120</sup> Therefore, new guidelines have to be authored, like, e.g., for the EU Directive on Electronic Money Institutions (Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions), cf. Electronic Payment Systems Observatory (ePSO) Newsletter – No. 7– May 2001; <http://epso.jrc.es/newsletter/vol07/welcome.html>.

<sup>121</sup> An overview on texts that deal with the developments in the area of "Electronic Cash" can be found at <http://www.ex.ac.uk/~RDavies/arian/money.html>; see particularly: Jim Miller: E-money mini-FAQ (release 2.0), Answers to Frequently Asked Questions about Electronic Money and Digital Cash; <http://www.ex.ac.uk/~RDavies/arian/emoneyfaq.html>.



**Figure 22: The Customer in the (E-)Banking Network**

### **Motivation for IMS**

In this scenario (cf. Figure 22), the IMS receives the function of dealing with the handling with various institutions in a secure, simple and privacy-compliant way. In contrast to other scenarios, the management of various pseudonyms for the purpose of anonymisation plays a less important role than the transparent management of various addresses with which a specific communication is desired but which belong to a common connection.

Further on, it would be conceivable that an IMA selects the institution with the currently most favourable offer for each transaction. This is not only economically rational but also positive as far as data protection is concerned because there would not be any complete or even central storage of all transactions in an extern place – provided that not every transaction requires the involvement of a third party instance. An IMA helps that from the complete data pool, only the data set which is relevant for the transaction with a particular institution is activated and released.

As long as an anonymous financial transaction is possible and called for in a data-protective way, it should be noticed and used by the IMA. It is still not foreseeable, though, which standard of digital money will actually have its way – particularly as far as the involvement of third parties.

### **Requirements**

**Table 5: Requirements of the E-Banking Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Management of addresses for specific financial transactions with corresponding histories, particularly for procedures which have not been fully settled; Pseudonym customer – finance office: identification as citizen; Pseudonym customer – house bank/mortgage bank/credit card bank/insurances: durable for duration of the contract; Pseudonym customer – trading system: transaction pseudonym
Usability	Easy to use because of usage by every normal customer
Security	Important, esp. prevention of identity theft and misuse; non-repudiation; prevention of accidentally false addressing

Privacy	Prevention of profiling; At the user's side: logging of the entire communication
Law Enforcement	Secure logging for the regulation of conflicts, demands for linkability because of the law on money laundering (if applicable).
Affordability	Cheap, for every-day use and every-person use

## 2.1.4 E-Government, E-Court and E-Democracy

There are a lot of different definitions of "E-Government" but no predominant one. For the study usable is the "Speyerer Definition" of Jörn von Lucke and Heinrich Reinermann of the Research Institute for Public Administration at the German Postgraduate School for Administrative Sciences in Speyer<sup>122</sup>. E-Government in this sense is the execution of business processes in connection with governance and government with help of information and communication technologies using electronic media.<sup>123</sup>

### 2.1.4.1 Tax Declaration

#### Description

The main actors in this scenario are the citizen who would like or has to make a tax declaration and the tax authorities that assign officials in charge to work on this tax declaration (cf. Figure 23).

The citizen receives receipts for settled transactions or services from various places (employer, bank, companies) (1). Those receipts are taken into account while making the tax declaration. The tax declaration is then sent to the tax authorities (2) that pass it on to a person in charge (cf. Chapter 2.1.2.3) who checks it formally and in content. The tax authorities will then calculate a tax assessment and send it to the citizen (3). Depending on this assessment, either the state transfers money to the citizen's bank account or the citizen pays the assessed liability via their bank (4).

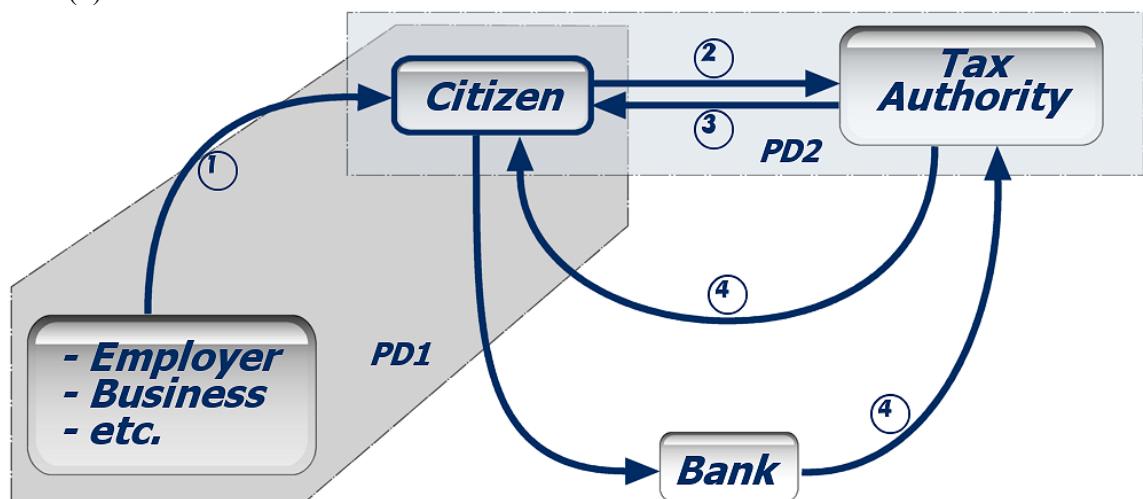


Figure 23: Pseudonym Domains of a Citizen in an E-Tax Scenario

#### Motivation for IMS

Both the state and the citizen have an interest in the assessment of the liability (including the acknowledgement or denial of tax benefits, depreciation etc.) without respect of the person. Furthermore, the citizen might want to prevent the state from collecting too many personal data

<sup>122</sup> <http://foev.dhv-speyer.de/ruvii>.

<sup>123</sup> "Unter Electronic Government verstehen wir die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien."

---

via the tax liability and being able to link to other circumstances. A completely automated tax declaration could accelerate the procedure which would result in a reduction of costs.

Pseudonym Domain 1 can exist between the citizen and third party persons and institutions that provide important information for the tax declaration (cf. Figure 23). These third parties confirm to having settled a certain transactions with the citizen without having to know any personal data on the citizen. On the one hand, it may be conceivable, though; that the third party uses a pseudonym to make sure the state cannot trace back the transactions. On the other hand, however, the state is interested in the prevention from abuse and therefore in the possibility to compare the statements of third parties concerning the citizen with those in their own tax declaration.

This pseudonym must remain valid for both the declaration at the tax authorities and also later for possible legal conflicts. Evidence of the citizen's expenses which they can optionally declare to save tax if possible do not have to be personal (as it is the case today). The only important point is that they can be handed in only once.

Pseudonym Domain 2 comprises the citizen and the tax authorities. By use of a pseudonym that is valid for only one tax declaration, the state could be prevented from building up long-term profiles of its citizens. On the other hand, the verification of the correctness of the declaration by comparisons over the years will be made difficult or even impossible.

For the case of tax depreciation over several years, it could be necessary to enable linkability to at least some items of the declaration.

The money transfer between the citizen and the authorities can take place by use of a pseudonym, though (Pseudonym Domain 3, cf. Chapter 2.1.3.3).

### **Requirements**

**Table 6: Requirements of the E-Tax Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Pseudonym I: durable for the tax declaration process until conclusion (perhaps until end of legal disputes), addressable by citizen Pseudonym II: durable for the tax declaration process until conclusion (perhaps until end of legal disputes), re-use possible for special tax advantages Pseudonym III: for money transfer (cf. Chapter 2.1.3.3)
Usability	Easy to use because of usage by every normal citizen
Security	Important, esp. for tax secrecy
Privacy	Prevention of profiling by state and business; At the user's side: logging of tax declaration for later disputes
Law Enforcement	Digital evidence necessary in case of identity theft, tax fraud
Affordability	Cheap, for every-person use one time a year

#### **2.1.4.2 Inquiry**

##### **Description**

Citizens' demands for information from public offices can have various aims. On the one hand, public records can be queried, information on stored data according to the Data Protection Acts or the examination of records according to the Freedom of Information Acts can be asked for. Depending on the kind, the information can be provided anonymously or only after identity verification and in connection with certain preconditions, e.g., evidence of personal interest or the affiliation to a particular professional group (e.g., notary).

In this context, the authorities also have to consider the interests of third parties or the information has to be permitted by those third parties. In some cases, the third parties can prevent the information or the permission for the examination of data.

In the sequel some main specific properties of three different types of inquiries are listed.

*Extract from the Register*

**Table 7: Properties with Respect to Extract from the Register**

<b>Examples</b>	Land register, trade register, residents' register
<b>Authorised to query</b>	Legitimate interests etc. Assumed for particular professional groups (e.g., notary)
<b>Identity verification</b>	Necessary
<b>Third parties</b>	Land owners, companies, residents

*Access according to Freedom of Information Acts*

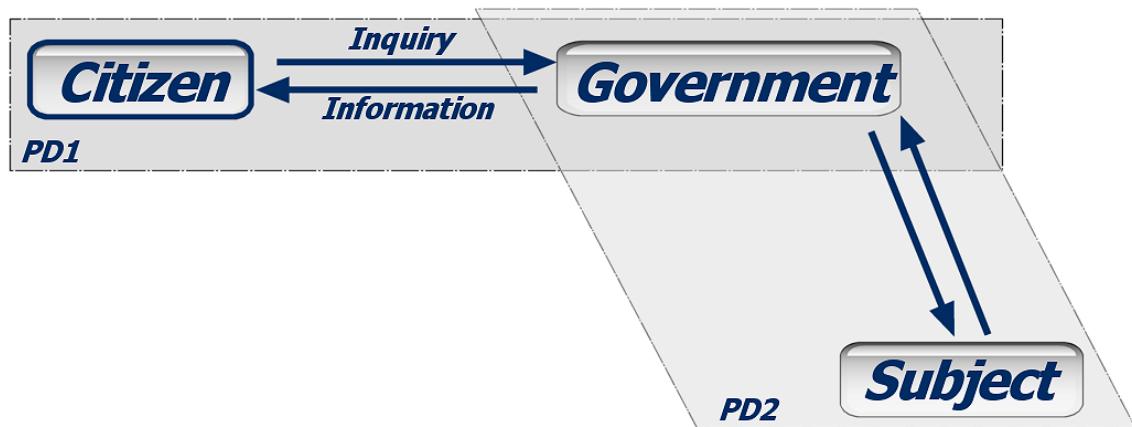
**Table 8: Properties with Respect to Freedom of Information**

<b>Examples</b>	Freedom of Information Acts, Public Affairs Law (Europe)
<b>Authorised to query</b>	Everybody, as long as there are no conflicts with public/third parties' interests
<b>Identity verification</b>	Not absolutely necessary
<b>Third parties</b>	Everybody mentioned in the records (land owners, companies etc.) and the public administration

*Access according to Data Protection Acts*

**Table 9: Properties with Respect to Access according to Data Protection Acts**

<b>Examples</b>	Information from any data processing party (cf. Directive 1995/46/EC Recital No. 41, 42)
<b>Authorised to query</b>	The person whose data have been processed
<b>Identity verification</b>	Necessary (if data stored under pseudonym: authentication by digital pseudonym appropriate)
<b>Third parties</b>	If the data of the relevant person are not separated from the personal data of others



**Figure 24: Pseudonym Domains of a Citizen in an Inquiry Scenario**

**Motivation for IMS**

Both the enquirer and third parties are interested in remaining anonymous. The enquirer can be interested in hiding their identity from the authorities to avoid disadvantages from the enquiry

---

but also from the third parties, e.g., to avoid disturbing the relationship within the neighbourhood.

The third parties can be interested in not letting the enquirer know if they permitted the information or not.

The use of rights on information is also of public interest (government observation) and serves the realisation of fundamental rights like the informational self-determination.

Recording the queries and information by the enquirer can be useful as it might serve a later derivation of legal claims. From the government's or a company's point of view, an omission of the documentation of such queries might be called for, according to the principle of data minimisation.

A long-term storage including the addressability of the enquirer could be called for if the documentation should be necessary for later queries or conflicts. A deletion should be carried out at the latest after the procedure has been finished. In the state administration directives, such deletion regulations currently exist for only few procedures.

Figure 24 shows the two main Pseudonym Domains: Pseudonym Domain 1 describes the relationship between the enquirer and the authorities. It can be limited to only one query but also connected with attributes or references to verify the right for a query. If the possibility of a verification is desired the pseudonym has to be addressable for a further time period. In case of a query on personal data, the relation to these data has to be proved. This would be easy if these data have been collected by use of the same pseudonym as deployed for the query. This pseudonym has to be clearly related to the enquirer who is to prove their identity as the pseudonym holder.

The Pseudonym Domain 2 describes the relationship between the third party and the authorities. It is possible to use a group pseudonym here, e.g., for all those concerned, that cannot be traced back directly to a third person.

### **Requirements**

**Table 10: Requirements of the Inquiry Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Pseudonym I: valid for the duration of the inquiry session until responding, addressable for receiving the requested information; In case of access to personal information: digital pseudonym Pseudonym II: valid for the duration of the inquiry session; group pseudonym possible
Usability	Easy to use because of usage by untrained users
Security	Important, esp. prevention of unauthorised access
Privacy	Prevention of profiling, anonymity of the citizen and the subject; At the user's side: logging of inquiry and response
Law Enforcement	Digital evidence necessary in case of identity theft, unauthorised access
Affordability	Cheap, for every-day use and every-person use Interest of the government

#### **2.1.4.3 E-Court: Civil Action / On-line Mediation**

##### **Description**

The main actors of this civil action e-court scenario are the plaintiff, the defendant, the court and the bailiff (cf. Figure 25).

The plaintiff or his/her lawyer institute proceedings at the court, which examines the statement of claim on the formal conditions and sends it to the defendant. The latter normally gets the possibility for a reply that will be passed on to the plaintiff via the court. Then the plaintiff can react again. After finishing this written procedure, the court appoints al hearing to which the plaintiff, the defendant, their lawyers, witnesses, experts etc. can be summoned. During the hearing, the arguments of both parties are exchanged, and a hearing of evidence takes place. Then the jury, normally composed of one or more judges, makes a decision, which will then be sent to both parties. As long as no appeal is lodged within a certain period, the decision can be executed. This can take place by the winning party putting a bailiff in charge of the enforcement. The bailiff then executes the charge at the other party. Money picked up during this procedure will be transferred to the client party.

Examples for existing on-line procedures comparable to a civil action are the arbitration procedures for disputes about domain names by the WIPO Arbitration and Mediation Centre, based in Geneva, Switzerland.<sup>124</sup>

The procedures of a civil action bear a partial resemblance to on-line mediation. Instead of a court, the mediator is resident between the two disputing parties. In contrast to a judge the mediator is not making a judgement. He is only acting as an intermediary between the parties and tries to find a compromise. A bailiff is not needed in a on-line mediation scenario.

The WIPO Arbitration and Mediation Centre provides on-line mediation for domain name disputes, too.<sup>125</sup>

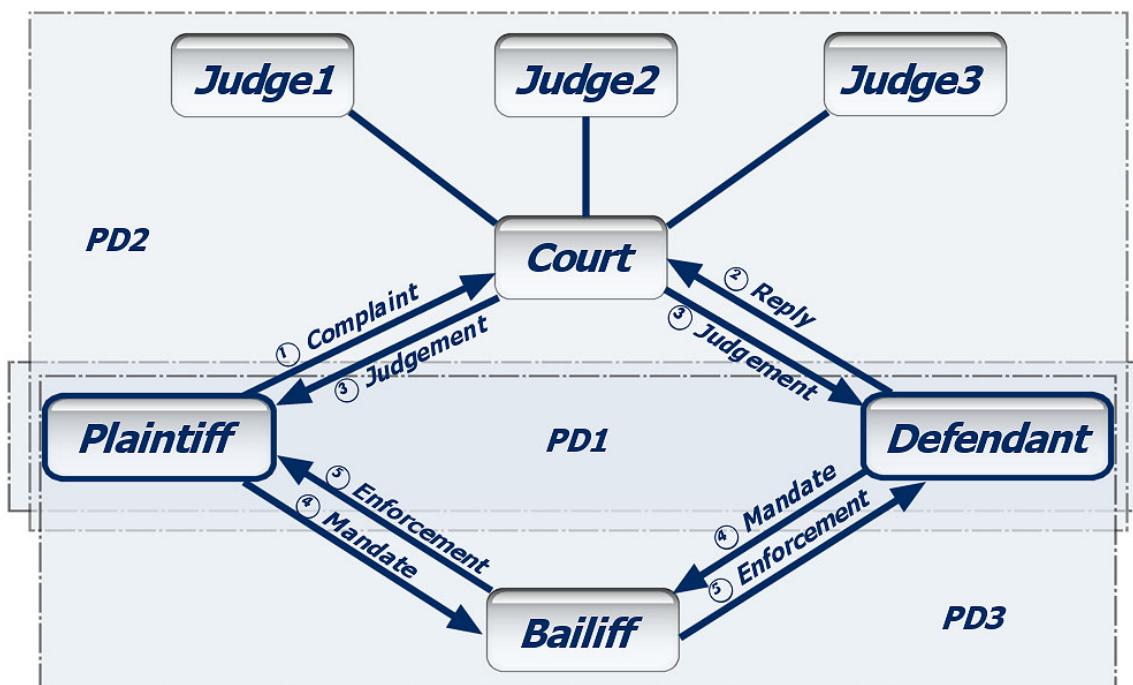


Figure 25: Pseudonym Domains of Plaintiff and Defendant in a Civil Action

### Motivation for IMS

Usually, hearings begin with taking down the particulars. It would be possible here to appear by use of a pseudonym. Such pseudonyms would have to meet certain requirements, e.g., at least if the accused is sentenced to jail they must be arrested as a person, i.e., the information behind the pseudonym would have to be revealed. However, there would be several possible ways that do

<sup>124</sup> <http://arbiter.wipo.int/arbitration/>.

<sup>125</sup> <http://arbiter.wipo.int/mediation/>.

---

not necessarily include a reference to the body of the accused. An example would be the arbitration in the area of on-line mediation.

Furthermore, a conceivable future would see personal pseudonyms that have an important meaning, i.e., a judgement could also refer to this representation of people. For example, authorisations that are linked to a pseudonym could be withdrawn, the judgement could influence the reputation of the pseudonym, or the use of the pseudonym could be completely prohibited (and technically prevented).

In cases of civil action, usually the plaintiff and the defendant as well as the public are interested in an independent judgement without respect of the person. In addition, both the plaintiff and the defendant could be interested in hiding their identity in the view of each other to avoid disadvantages in the daily life outside the lawsuit.

The Pseudonym Domains are shown in Figure 25. Pseudonym Domain 1 exists between the plaintiff and the defendant. This pseudonym can only be applied to one court procedure, independent from other proceedings, to prevent aggregation of information drawn. It must be addressable by both the other party and the judge to influence the lawsuit. It must also remain valid for higher courts.

Legal Action during which the defendant and the plaintiff appear using pseudonyms in the view of each other are only conceivable in conflicts that are independent from a personal relationship (examples for personal relationship: family, neighbours, employer / employee, victim / offender).

Pseudonym Domain 2 comprises the plaintiff, the offender and the court. This domain is decoupled from the relationship between the two parties in conflict who might know each other. In order to preserve the court's independence and objectivity, all documents and pieces of evidence will be passed on by use of pseudonyms, if applicable. This is particularly conceivable in cases which do not require the personal appearance of the parties (cf., e.g., the German summary procedures, available for claims for a specified sum or quantity, where the plaintiff relies entirely on documentary evidence).

Pseudonymised data could be made available for expert testimony in order to achieve neutral results, as long as a personal examination is not necessary.

Pseudonyms remain addressable for queries and higher courts until a decision is final.

On-line mediation needs only one Pseudonym Domain between the two parties and the mediator. For a successful mediation it is necessary that the mediator is included into the communication between the parties and can interact with them.

## **Requirements**

**Table 11: Requirements of the Civil Action Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Pseudonym I: durable for the civil proceedings until final judgement, addressable by other party Pseudonym II: durable for the civil proceedings until final judgement, addressable by the court, could be needed to be revealed for enforcement
Usability	Easy to use, but could be more complex in case of use by lawyers
Security	Important, esp. prevention of identity theft
Privacy	Prevention of profiling, anonymity of parties for public in general; At the user's side: logging of pleadings
Law Enforcement	Digital evidence could be necessary for civil action itself or later proceedings
Affordability	Within the limits of the normal fees by court

### 2.1.4.4 E-Court: Criminal Proceedings

#### Description

In cases of criminal proceedings<sup>126</sup>, the public prosecutors carry out investigations concerning the accused party in the preliminary examination. If they come to assume that a crime has been committed the prosecutor moves for an issue on criminal action at the court. If the court considers a condemnation to be possible, a criminal case will be instituted. The accused will be informed and they will be allowed to make a statement upon the accusation. A trial will be appointed to which the accused, possible co-plaintiffs, witnesses, experts, lawyers etc. will be summoned. The case will be tried based on statements from the prosecutor and the accused, and a hearing of evidence takes place. Then the court, which usually consists of one or more judges and sometimes law assessors, makes a decision of which the accused, the co-plaintiffs and the prosecutor will be informed. If none of the people involved lodges an appeal the decision will be executed then.

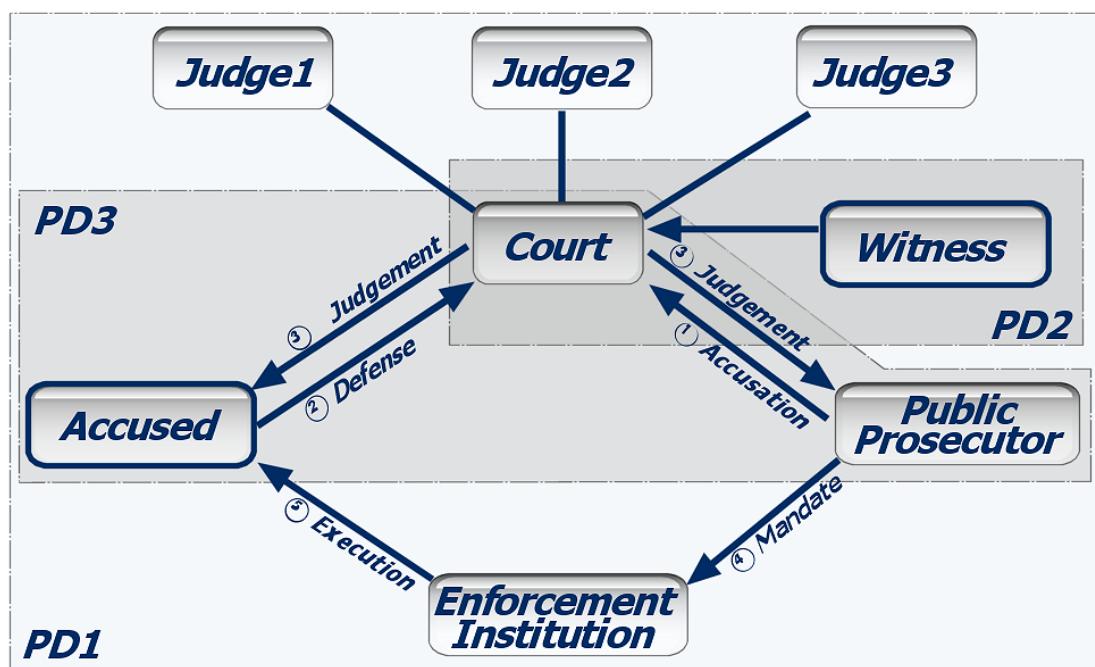


Figure 26: Pseudonym Domains of Accused and Witness in Criminal Proceedings

#### Motivation for IMS

By using pseudonyms (cf. Figure 26), the objectivity of the court and the prosecutors can also be achieved in cases of criminal proceedings. In addition, it saves the reputation of the accused from being damaged.

Most of the legal systems of the world know the principle of public trial. This means that at most legal proceedings the public has the right to be present. Exceptions are, e.g., family trials and trials relating to young offenders. The reason for this principle is that the public should control the court to assure that everybody is treated equally under the principles of a fair trial. This means that one aim of the principle of public trial is to protect the accused. Trials are imaginable where the accused is interested in not being anonymous due to the trial. It must be possible for the accused to decide if he wants to act under a pseudonym not known by observers or not.

<sup>126</sup> Criminal proceedings are nation-specific. Considering here Germany as an example.

---

The pseudonym should remain valid as long as the trial lasts, until the decision is final, and possible penalties have been completed. Up to then, it must be possible for the accused or the prosecutor (appeal) and the court to refer to the accused person until completion of the execution of the sentence. Shorter validity duration is only conceivable if the execution of the sentence refers directly to the pseudonym by, e.g., withdrawal of certain rights. This again would be only conceivable if the penalty refers to the pseudonym only (e.g., in a lawsuit on a traffic offence, the accused uses the driving licence as a pseudonym – the licence is directly connected to the permission to drive and its limitations).

Another Pseudonym Domain exists between the court and witnesses who need a particular security in the view of the accused. In these cases, it must be impossible for the accused to get to know the real identity of the witnesses or to put them under pressure, but at the same time, they must be able to defend themselves against the pseudonymised statements made by the witnesses. This pseudonym has to remain valid until the court's decision is final to enable examinations and queries.

### **Requirements**

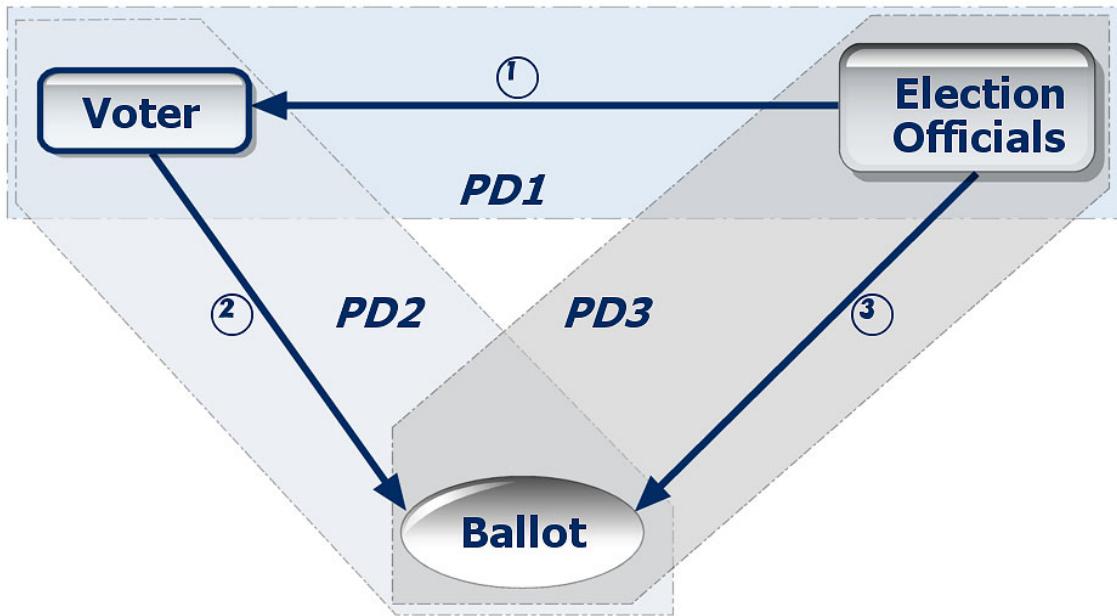
**Table 12: Requirements of the Criminal Proceedings Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Pseudonym I: durable for the criminal proceedings until final judgement, addressable by defendant, court and public prosecutor; Possibility of the accused to use real name; Pseudonym II: durable for the criminal proceedings until final judgement, addressable by court and public prosecutor, limited by defendant, can be revealed for penalty if this refers to the person himself
Usability	Easy to use, but could be more complex in case of use by lawyers
Security	Important, esp. prevention of identity theft
Privacy	Prevention of profiling, in particular anonymity of the defendant for public in general; At the user's side: logging of pleadings and whole trial
Law Enforcement	Digital evidence necessary for proceedings itself or later proceedings
Affordability	Within the limits of the normal fees by court

### **2.1.4.5 E-Voting**

#### **Description**

In a voting scenario (cf. Figure 27), each authorised voter first gets the ballot paper from the election officials (1). The right to vote may depend on specific properties, e.g., being of full age. Normally it should be conducted as election by free and secret ballot; each voter has only one vote. In a predefined time frame the voters put their ballot papers into a ballot box where all votes are collected (2). After closing of the polling places, the election officials perform a controlled procedure to open the ballot box and count the votes (3).



**Figure 27: Pseudonym Domains of a Voter in an E-Voting Scenario**

### Motivation for IMS

Voting is not a typical scenario for identity management since there are barely degrees of freedom for the user in managing his or her identities. Furthermore, the tradition of free and secret ballots already demands

- Authentication of the voter before he or she votes and
- Anonymity and unlinkability of votes with respect to voters after casting of votes.

Translating the traditional concept of voting for the digital world, compatible requirements have to be met. IMS could be used for identification and authentication with respect to the election officials, to store "e-ballot papers" for coming elections and for voting itself in an anonymous environment. The Pseudonym Domains signify the different situations in the election context, each of them being characterised by specific properties (cf. Figure 27): In Pseudonym Domain 1 the voter – possibly including demanded attributes – has to be identified and authenticated to get the ballot paper; in Pseudonym Domain 2 the voter has to be – possibly pseudonymously by the ballot paper – authenticated as well to cast his or her vote; and in Pseudonym Domain 3 only anonymous representations of the voter's will in form of votes can be seen by the election officials without the option of linking them to the original voter again. The votes can be regarded as transaction pseudonyms, only valid for a specific election procedure, limited to one per voter, with or without the possibility of transferring them to other people.

### Requirements

**Table 13: Requirements of the E-Voting Scenario**

Category	Characteristics and substantiation
Functionality	Pseudonym I: durable until completion of election, identifying and authentication of voter, possibly include demand attributes; Pseudonym II: durable until completion of election, authenticated to cast vote; Pseudonym III: durable long time for later verification, no linking to original voter
Usability	Easy to use because of usage by every citizen (at least adults)
Security	Very high demands, important for society
Privacy	Preservation of secrecy of the ballot; Anonymity of the environment
Law	For prevention of electoral fraud

Enforcement	
Affordability	Paid by society

## 2.1.5 E-Health

### 2.1.5.1 Description

The health system as a whole generates a network of relationships of various kinds between a large number of parties. An international comparison shows that the numbers of these parties and their relationships differ quite a lot.<sup>127</sup>

However, there is a connection concerning the accounting and research between the parties/processes that are directly connected with the treatment of patients. For example, a doctor charges a treatment to a private patient's account, the patient pays the bill and sends it to the health insurance company in this explicit form for refund. Therefore, the insurance company may get more or less a complete record and profile of the patient's health condition. For patients with a compulsory health insurance, the doctor sends his claims for payment in pseudonymised form to the association of compulsory health insurances which then collects the demands of all patients from the corresponding insurance companies. If the doctor diagnoses an illness that is included in the epidemics law he has to report it to the public health office. On this basis, the public health office creates statistics on the distribution of certain diseases. In addition, both the patient and the doctor can volunteer in research projects.

### 2.1.5.2 Motivation for IMS

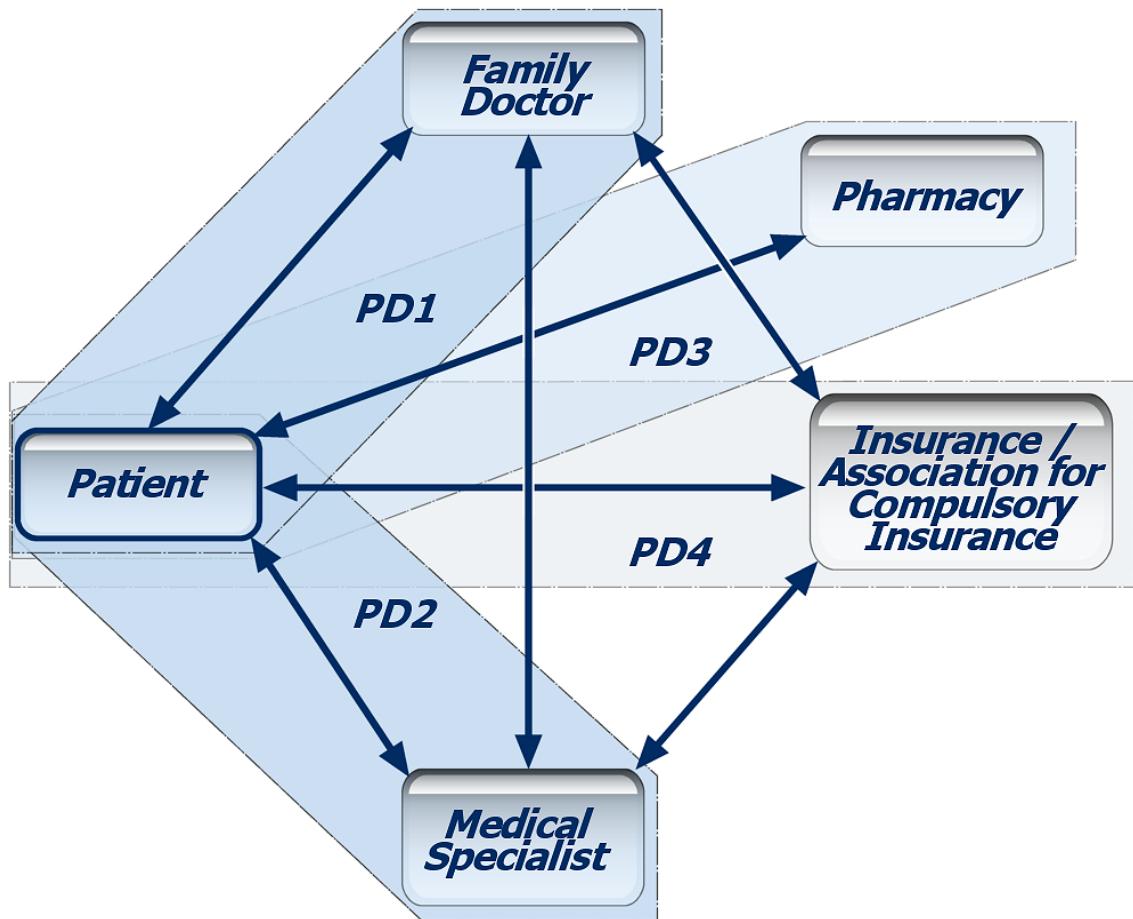
The motivation for the use of an e-health-related IMA consists in the possibility for the patients to document their own health history completely and to use the relevant aspects for a treatment. This documentation can – at least theoretically – be carried out particularly privacy-compliant. The result will be an increased transparency, e.g., of risks concerning X-rays, pain killers or antibiotics, and maybe a cost reduction as repeated examinations can be dropped or are at least documented as such – which may lead to economic sanctions in cases of unnecessary examinations.

In general, a de-personalised pre-step of a binding diagnosis can take place via telephonic advice. This will lead to a cost reduction and the improvement of privacy protection. Such anonymous advice calls have already been offered for some years by health insurance companies or special information centres for advice on socially problematic diseases (drugs, HIV). It is foreseeable that such interactive and also anonymous advice could be possible via the Internet. Current scenarios on the modification of the health system predict a well-informed sovereign patient [cf. PWC 2002].

The special confidential relationship between the patient and particularly the family doctor is manifested in the control of records. A doctor who keeps these records takes the position of the family doctor and does some sort of identity management for the patient (in the sense of an Identity Protector (cf. Chapter 2.1.2.2)) in the view of other institutions involved. The family doctor serves, e.g., as a pseudonymising entity when dealing with a laboratory or a research institute (and describing the case in an abstract way) or another doctor (when seeking advice). This constellation of an identity management on behalf changes when the patients manage their own files on their own. In this case, the advantages of an IMS can be made use of because the specific communicative requirements to the corresponding institutions with which the patients interact can be managed by the IMA. The complexity of the individual workflow between the patient and the institutions is illustrated in the graphics shown above. If a patient keeps their own file an aspect to be specially treated could be the definition of the modalities by which the data currently generated by the doctor will be added to the file documented by the patient. In

<sup>127</sup> Pressestelle und Verlag der Österreichischen Ärztekammer, n.d.: "Vergleich: Gesundheitssysteme in der EU"; Wien; <http://www.aek.or.at/EUSTUDPPT/systeme.html>.

spite of the control of the complete file, the patient's autonomy is limited, as the family doctor takes the additional positions of a translator of special findings and of a mentor who attends to the patient psychologically, socially and with regard to time and the account. Another special aspect of the use of an IMA for e-health is the necessity of making provisions for the case that a patient is not able to use the IMA in an emergency case or that someone loses their IMA. The latter is a problem that can be solved by the general implementation of an IMS. A possible solution might be to include the archiving of IMA backups in the core area of state responsibility. But it might also be possible to think about a private sector solution.



**Figure 28: Pseudonym Domains of a Patient in an E-Health Scenario**

A strongly simplified scenario looks like this: A person is in acute pain, cannot help himself/herself and – in the typical manner – consults the family doctor. The family doctor makes a first diagnosis on the basis of an already existing patient dossier and possibly of another, more detailed diagnosis made by a specialist or refers the patient to the specialist. Successively, the therapy will be defined. According to the German law, each of the doctors who work with the patient is bound to keep a patient-related documentation. Exceptions may only be made in urgent cases like accidents etc. The eventual payment takes place by paying the insurance policy and the appropriate fees and accounts with the insurance company. In such a constellation, an IMA could help the user to keep their own patient dossier created by the doctor, including all applied medicaments and consultations. The doctors in charge will naturally keep their own files, particularly when dealing with speculations that are related to the patient but of which they shall not know, e.g., notes on speculations on a diagnosis that have been made too early to be revealed to the patient. The most important aspect is, however, that the user is basically able to decide by himself/herself which institution is to receive which information. Particularly the official data that legalise an account must be passed on to the patient dossier. While the normal relationship between the patient and the doctors is assumingly always confidential and very personal, the account can be processed largely in a pseudonymous way, like in many other cases.

---

## **Requirements**

**Table 14: Requirements of the E-Health Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Data warehouse, opportunity of the integration of a process across the various areas of procedure (healing, account, research); Pseudonym I: long durability, re-use for further examinations; Pseudonym II: durable until end of examination; Pseudonym III: transaction pseudonym; Pseudonym IV: durable for duration of the contract
Usability	High demands; particularly on the support of which (amount of) data are to be made accessible to a doctor
Security	High demands: It is to be considered if there is to be an entity that is to keep a backup of an IMA. In addition, a procedure for emergency cases in which the patient is not able to give access to data has to be defined.
Privacy	High demands (according to Art. 8 EU Privacy Directive, medical data are to be considered as particularly sensitive) since the complete biographical data will be present in a case of abuse. This means a segregation of the different areas of procedure in particular. At the user's side: logging of all communication
Law Enforcement	Secure logging for the processing of conflict
Affordability	Cheap, for every-day use and every-person use

## **2.1.6      Miscellaneous**

### **2.1.6.1      E-Science: Review Process of Articles**

#### **Description**

The author delivers an article to the editors (1) who are responsible for a formal evaluation. If the editors accept an article for publication, they forward it to the reviewers (2) who evaluate the content. They give feedback on the text to the editors (3) who send the reviewers' comments to the author (4). After revising the text, he sends it back to the editors (5). If they regard the article as finished, they send it to the publishers (6) who publish the text.

Traditionally editors ensure by organisational means the author's anonymity against the reviewers and/or the reviewers' anonymity against the author. This reflects society's interest in freedom of science (cf. Art. 13 Charter of Fundamental Rights of the EU) and in freedom of speech (cf. Art. 11 Charter of Fundamental Rights of the EU) by supporting fairness in the evaluation process.

On the other hand after the reviewing process, the author normally does not stay anonymous any more: By using his name or a chosen pen-name in his publications he establishes a reputation, e.g., according the academic tradition.

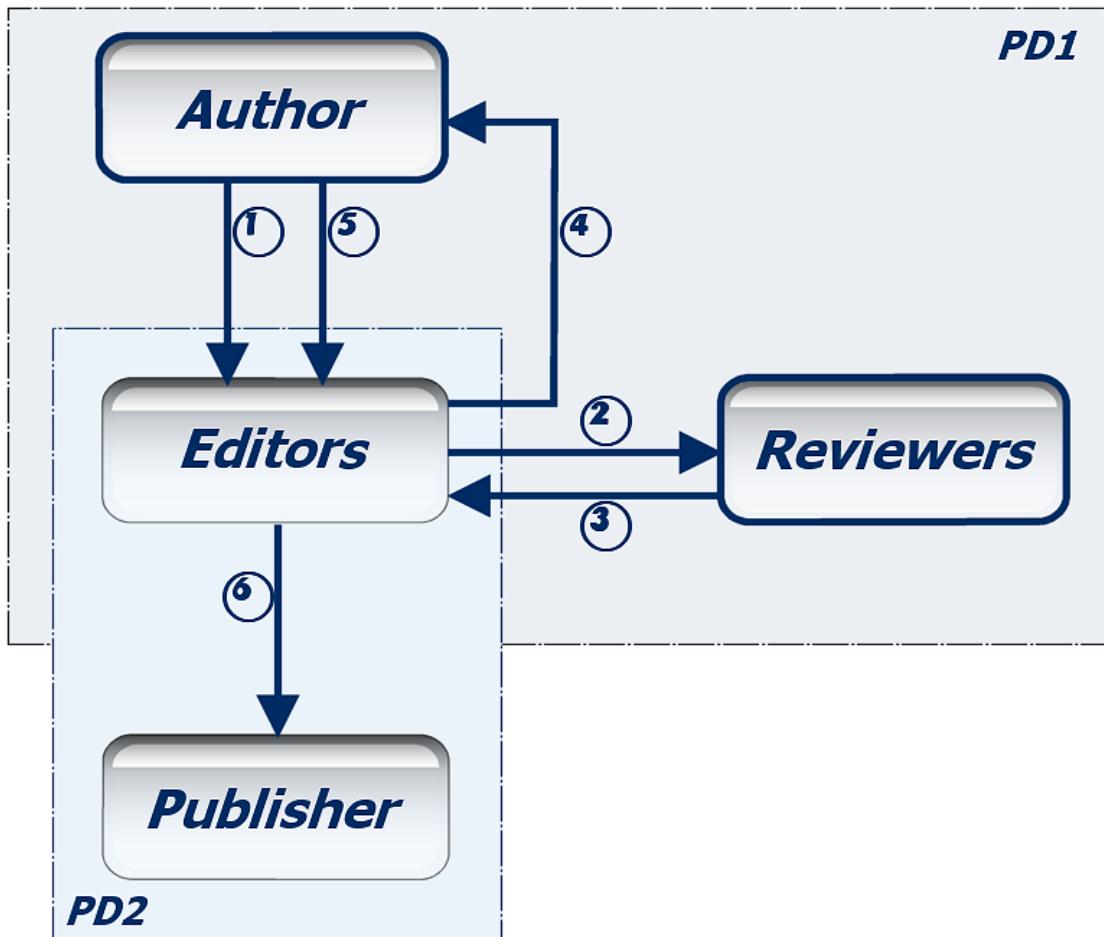


Figure 29: Pseudonym Domains of Author and Reviewers in a Review Scenario

### Motivation for IMS

IMS can be used to technologically implement the tradition of anonymity in the review process and in some cases even enhance today's state-of-the-art. Figure 29 shows two de-coupled Pseudonym Domains, which represent different stages in the review process from the author's point of view:

- Pseudonym Domain 1 describes the process of text evaluation where the author can use a pseudonym from the beginning on, i.e., delivering the text to the editors until handing over the revised version according to the reviewers' comments. Thus, he may stay anonymous against both reviewers and editors, if so desired.
- In Pseudonym Domain 2, the author can be known by a different pseudonym (or his real name) under which his text is published.

The author's anonymity even against the editors may support equal treatment without distinction of person.

### Requirements

Table 15: Requirements of the Review Scenario

Category	Characteristics and substantiation
Functionality	Pseudonym I: durable for the transaction until finishing article, addressable by the editors Pseudonym II: long durability, re-use possible to establish reputation; If possibility of discussion desired: addressable pseudonym; If one should be able to call the author to account: e.g., traceable pseudonym

Usability	Also more complex usage bearable because users are professionals and well-skilled
Security	Integrity important, esp. prevention of reputation theft and plagiarism, i.e., authenticity and in some cases also non-reputability desired
Privacy	Anonymous publication if desired: no linkability between text and author
Law Enforcement	Digital evidence necessary in case of plagiarism, identity theft, reputation theft, unlawful content ...
Affordability	Indifferent: a) Professional process b) Interest of society

### 2.1.6.2 E-Notary / E-Witness

#### Description

The role and definition of electronic notarisation is to be a qualified witness. The E-Witness supports the trustworthiness of a given transaction by

- a) Identifying the interacting parties;
- b) Verifying "who" "did what" and "when" in an electronic interaction on a network;
- c) Increasing the overall trustworthiness so that a legal dispute can be prevented;
- d) In case of a dispute, providing indisputable evidence the conflict resolution.

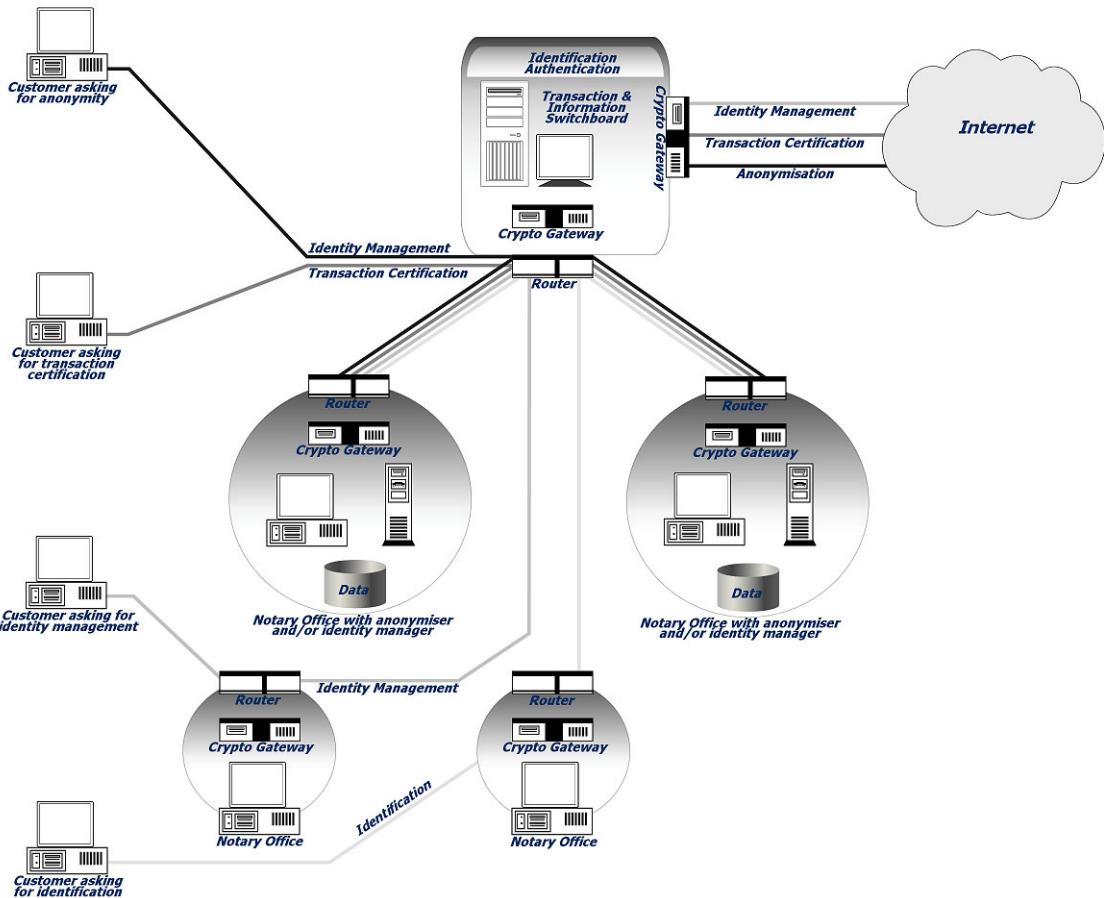
Considering that the notary in the Latin notary system (utilised by about 100 legal systems around the world) is a qualified witness of a legal transaction, we distinguish between two kinds of electronic notarisation:

1. The e-Witness: The witness is performing the same functions as a public notary, but is not a public official according to the legal system applicable. So the transactions witnessed by it have no privileged legal value.
2. The e-Notary "strictu sensu": In this case the electronic witness is a public notary according to the legal system applicable. This scenario is quite visionary because the existing legal regulation of the notary activity in countries, in which there are Latin public notaries, requires the presence of the parties in front of the notary. Nonetheless it is conceivable that with proper control on the technical means of the electronic transaction, in cyberspace the link of time and space required by existing notary legislation in Europe will be digitally re-created.

#### Motivation for IMS

The notary is an impartial witness of the transaction. If the public has to be engaged with confidence in e-Commerce transactions, safety and security must be guaranteed and credibility preserved. However, e-Commerce through open communication networks and digitalisation involves a set of problems quite different from "real" transactions.

Considering that a public notary is a public official in the countries, which adopted the system of Latin notary, it is conceivable that the public notary takes also the functions of IMS providers, offering pseudonymity or anonymity to the identified parties on demand. In this case it is more likely that the legal system will accept pseudonymity and anonymity as a non-threat to legal security. In fact legal systems where Latin notaries are recognised public officials, already give to the notaries the duty to handle relevant and privileged legal information confidentially.



**Figure 30: Integration of Notaries as E-Witnesses**

Figure 30 gives a detail of how geographically distributed servers may interact in managing personal data and transaction evidence.

A customer requests an electronic identity from a public notary to be given (bottom left of the figure). This happens through the use of a qualified signature creation device. The customer can present it to the notary or the notary will issue on demand, acting as a registration authority of some certification authority issuing qualified certificates (according to the definition of the Directive 1999/93/EC).

The notary asks the central data switch to be given a serial number for the given identity (pink link between the notary and the crypto gateway of the switchboard). The central switchboard keeps only evidence of the request of a serial number, but no personal data. These can be distributed among several geographically distributed servers managed by notaries. The switchboard keeps a record of this operation, again without access to the personal data of the person identified by the notary.

From this moment the customer has a trustworthy identity that can be kept fully anonymous or operate under a pseudonym. Only the gatekeeper of the system is able to verify and bring together the different transactions to a serial number. None of the gatekeeper is able to know who is behind the given serial number, because only the first identifying notary knows.

The interesting fact is that Latin notaries already fully rely on identifications carried over worldwide by other notaries. So there is nothing new in the full trust given to a single identification provided by a colleague. In this case there are even more information on the identification process than in any current case of legalised proxy or notary deed. The system simply transposes in digital environment what already happens in legal environment, taking advantage

---

of the possibilities of the digital means in order to protect personal data and improve the information available, at the same time.<sup>128</sup>

## **Requirements**

**Table 16: Requirements of the E-Witness Scenario**

<b>Category</b>	<b>Characteristics and substantiation</b>
Functionality	Identifying the interacting parties, verifying "who" "did what" and "when" in an electric interaction on a network
Usability	For usage by normal customers
Security	High demand on integrity, confidentiality and availability of IMA and e-witness (reliability of service; "what you see is what you sign")
Privacy	Prevention of profiling, logging of attestations
Law Enforcement	Digital evidence with high probative value
Affordability	For important business with very high security / probative value more expensive than for every day usage

### **2.1.6.3 Location Based Services**

#### **Description**

Location based services (LBS) are a growing business area of mobile network operators. As many people possess a mobile phone, they can use those personalised services based on location. One distributed technology for positioning is the Global Positioning System (GPS). Additionally network based positioning by means of triangulation of the signal from cell sites serving a mobile phone may be used. The location data is mostly interpreted in conjunction with Geographic Information Systems (GIS).

There are four major categories of LBS:

- Location based information:  
An example for such a personalised services is the search for restaurants or hotels within a certain proximity to the mobile user.
- Location based billing:  
The user can establish personal zones such as a home zone or a work zone to enjoy special rates.
- Emergency services:  
In emergency calls the location of the caller may be disclosed to the appropriate authorities. In the United States of America, the FCC has mandated that by October of 2001, all wireless carriers in the US must provide a certain degree of accuracy in pinpointing the location of mobile users who dial 911.
- Tracking:  
An example for such an application is tracking vehicles for purposes of the owning company knowing the whereabouts of the vehicle and/or operator. Furthermore mobile user could be tracked for many purposes, e.g., for notification of a sale at a store close to the user's current proximity.

#### **Motivation for IMS**

The IMA could help the user in managing his or her mobile service including the location based services. Thus, not only reachability management or address management would be reasonable,

---

<sup>128</sup> EASET (European Association for the Security of Electronic Transactions) is organising itself as a Groupement Européen de l'Intérêt Economique (GEIE) that operates under the Law of Luxemburg. It is formed to provide notary trust services in digital environment, combining in a striking innovative way existing open (and open source) technology. European Notaries from Austria, Belgium, France, Germany, Italy, Luxembourg and Spain and also committed and experienced business people and IT specialists form EASET (<http://www.easet.net/>).

but also a kind of location management. In this case main management functionality would be to enable or disable the provision of location data. Also the resolution of location data could be configured.

In today's networks even without transferring explicit location information, with some effort the mobile service operator can find out a quite exact location if the mobile phone is switched on. Real anonymous mobile services are not state-of-the-art, although there have been concepts since a few years how to design mobile network architecture for gaining anonymity for the users or even how to enhance the existing network structure for applying some anonymity functionality [cf. Federrath 1999a, 1999b]. It is remarkable that a ubiquitous scenario where all things may have senders and sensors may be more privacy-friendly than the mobile phones because they could communicate directly with the user or his/her devices and not via central network providers.

At least the IMA could support the awareness of the user who might find out what (location) data about him or her.

### 2.1.7 Conclusion

**Table 17: Summarisation of Requirements of Scenarios**

Category	Characteristics and substantiation
Functionality	<ul style="list-style-type: none"> <li>The specific functionality for each scenario has to be fulfilled like <b>identity administration, gateway, notice and control</b></li> <li><b>Identity Administration</b> <ul style="list-style-type: none"> <li>- Transaction pseudonym</li> <li>- Group pseudonym possible</li> <li>- Addressable pseudonym</li> <li>- Traceable pseudonym</li> </ul> </li> <li><b>Gateway</b> <ul style="list-style-type: none"> <li>- Handling of communication between user and other parties</li> </ul> </li> <li><b>Notice</b> <ul style="list-style-type: none"> <li>- Pseudonym possibly <b>durable</b> for different kind of actions</li> <li>- Identifying the interacting parties, verifying "who" "did what" and "when" in an electronic interaction on a network</li> </ul> </li> <li><b>Control</b> <ul style="list-style-type: none"> <li>- Pseudonym <b>addressable</b> by organisation</li> <li>- <b>Re-use</b> of pseudonym possible for special advantages / <b>establish reputation</b></li> <li>- Possibility of reliable <b>re-pseudonymisation</b> / identification</li> <li>- Possibility to <b>use real name / identity</b></li> </ul> </li> </ul>
Usability	<ul style="list-style-type: none"> <li><b>Basic usability</b> for all participants in the system, being implemented in system design, documentation, and possibly support, is a mandatory requirement.</li> <li><b>Easy to use</b> because in case of usage by every normal customer / untrained users</li> <li>Could be more complex in case of use by <b>professionals</b></li> <li>Also more complex usage bearable when users are professionals and well-skilled</li> </ul>
Security	<ul style="list-style-type: none"> <li><b>Availability</b></li> <li><b>Integrity</b></li> <li><b>Confidentiality</b></li> <li>As far as sensitive data are concerned, confidentiality measures should be taken.</li> <li><b>Prevention of identity theft, reputation theft and misuse</b> of, e.g., credit card numbers; non-repudiation; prevention of accidentally false addressing</li> </ul>

	<ul style="list-style-type: none"> <li>Prevention of <b>manipulation</b>; non-repudiation</li> <li>Prevention of accidentally false addressing</li> <li><b>Prevention of unauthorised access</b></li> <li><b>Prevention of plagiarism</b>, i.e., authenticity and in some cases also non-reputability desired</li> <li><b>Reliability of service</b>; "what you see is what you sign"</li> </ul>
Privacy	<ul style="list-style-type: none"> <li>The <b>legal requirements</b>, which can differ in the various scenarios, have to be fulfilled.</li> <li><b>Prevention of profiling</b> by organisation / companies</li> <li>Possibility of <b>anonymity</b> of the user</li> <li>At the user's side possibly <b>logging</b> of the relevant communication (inquiry and response)</li> <li><b>Prevention of linkability</b></li> </ul>
Law Enforcement / Liability	<ul style="list-style-type: none"> <li>The <b>legal requirements</b>, which can differ in the various scenarios, have to be fulfilled. In some cases there may be no need for extra law enforcement requirements, e.g., because the IMS is used in legally non-relevant communications or because a misuse cannot happen. Generally speaking for providing fair transactions either there has to be a performance bond of the contract or there should be enough significant digital evidence to prove one's position in court.</li> <li>Possibly requirement of <b>linkability</b> in the organisation office</li> <li><b>Digital evidence</b> necessary in case of identity theft, reputation theft, warranty (e.g., receipt), wrong delivery, tax fraud, unauthorised access, civil action ...</li> <li><b>Secure logging</b> for the regulation of conflicts</li> <li>Digital evidence with <b>high probative value</b></li> </ul>
Trustworthiness	<ul style="list-style-type: none"> <li>Measures for objective trustworthiness of the IMS (by implementing usability, security, privacy and law enforcement functionality where appropriate) should be taken, supported by measures for gaining trust.</li> </ul>
Affordability	<ul style="list-style-type: none"> <li>The integration of identity management functionality should not make transactions far more expensive than the actual one. If possible, by integration of this functionality the participants also strive for additional economical advantage by creating new business models and services.</li> <li>Cheap in case of <b>every-day use</b> and <b>every-person use</b></li> <li>Usage could be in the Interests of the <b>government</b></li> <li><b>E-Court</b>: within the limits of the normal fees by court</li> <li><b>E-Government</b>: maybe paid by society</li> <li>For important business with very high security / probative value more expensive than for every day usage</li> </ul>
Interoperability	<ul style="list-style-type: none"> <li>The new functionality should be both compliant to legacy systems and to new standards.</li> </ul>

The diversity of scenarios demonstrates use cases for identity management and IMS. The degree of anonymity may vary: In some cases the user can remain anonymous, in other contexts identification is necessary or desired. Sometimes self-authentication is sufficient, e.g., in reputation systems, in other cases external authentication is needed by getting certificates from organisations. Specific functionalities are role management, address management, reachability management, and location management. IMS even has central facets of risk management.

In Chapter 1, the general liberality of law with respect to identity management including anonymity and pseudonymity has been highlighted. In the current section, certain scenarios reveal that many specific requirements derived from specific legal regulation, from traditions or from legacy systems restrict the degrees of freedom of identity management.

The scenarios are Gedankenexperiments to estimate possibilities for IMS. The added value of IMS and possible substitutions in the given scenarios needs to be analysed, e.g., for which parts legal or societal changes would be necessary and where specific technological or infrastructural support has to be provided. For instance in order to accommodate pseudonymous tax declaration, some national regulation would need to be adapted, a cost-effective distributed pseudonymous electronic signature infrastructure, which does not impose additional obligations to the user, would be helpful. In an IMS-enhanced world where pseudonymous digital receipts are established practise, a tax declaration could be handled without media conversion (and without "identity conversion").

Some general structural elements can be identified: Pseudonym Domains define scopes of different pseudonyms which may be used in successive or concurrent phases of a scenario, e.g., beginning with anonymous access for browsing without obligation, changing later on to legally binding transactions with other pseudonym use. Additionally in some scenarios entities for separating and linking pseudonyms between different parties are integrated, acting as Identity Protectors on behalf of the user. The traditional workflow often consists of such entities, but in future they will become less important with user empowerment by end-to-end security and IMS.

## 2.2 Main Requirements

As shown in Chapter 2.1, the following requirements are relevant to IMS.

### 2.2.1 Functionality

Taking into account the views of all actors an Identity Management System should fulfil specific functionality: It should help the user to manage his identity. Considering identity management, we distinguish between a general, beforehand *identity administration* which is independent from current communications and the management of identities during specific communications and situational contexts. For the latter, it is necessary for the IMA to have interfaces to the communication partners, especially to digital networks. This *gateway* functionality also restricts the influence the IMA may have (cf. Chapter 1.2.3). Management always is defined as taking decisions basing on *notice and control*. These requirements apply to the process of identity management, i.e., informing the user about a situational context and offering choices if appropriate.

This means in more detail:

- a) Identity administration:  
The IMA has to provide the possibility to administrate the partial identities and identity data, i.e., handling and representation of identities. The technical processes for creating the data set entry and updating or deleting it on demand have to be implemented. This data set entry may also comprise digital signatures, certificates, or credentials.
- b) Gateway:  
The IMA can act as gateway for digital communication. Thus it has to provide functionality to manage data exchange with all communication partners.<sup>129</sup>
- c) Notice and control:  
The core property of IMA is the option of choosing partial identities as required or desired

---

<sup>129</sup> Identity Management Applications incorporate gateway functionality by definition, because identity management is always a process between the user and another party. Of course not all other functions rely on communicating with the outside world, e.g., administering own identity data could be handled off-line. But the appearance of a user under different pseudonyms regardless of the type of communication partner requires that a communication line has been established, and this is one of the tasks of an Identity Management Application. As the gateway functionality is inherent in an IMA and as standard interfaces and mechanisms from other applications such as browsers or e-mail clients are mostly used for this purpose, the gateway functionality was not tested and evaluated as such in this study.

in a specific context and situation. Firstly the user has to be aware of context and situation. This may comprise information about the communication partner, about the role the user is acting in, about former transactions, about the conditions for data exchange. This transparency function is necessary for an informed choice which data to transmit and for a later examination of data exchange. Secondly the user should be able to control when to release which personal data to whom. The process of choosing partial identities and identity data can be explicit, e.g., by asking the user in a pop-up window, or the desired behaviour of the IMA can be pre-defined in policies which contain rules on the decision between partial identities or act according to default values. External information may be integrated in this process of choosing personal data as well.

Of course IMS functionality requires appropriate interfaces for the communication with the user (mostly graphical user interfaces (GUIs)) and with other applications or protocols (Application Programming Interfaces (APIs)).

For service providers and IMS providers, the basic functionality requirements do not differ to a large extent from the users'. Adjusted to the kind of organisation, special functions of the aforementioned list become more important than others. Typically, organisations will have to manage members' and associates' identity information, thus different kinds of identities. Functions for controlling this complexity and keeping it up-to-date are part of the main basic requirements of functionality.

## 2.2.2 Usability

Two models have emerged within the last decade, which provide a strong theory base for studies of utilisation behaviour: the Technology Acceptance Model by Davis [cf. TAM 1985] and the Task-Technology Fit Model by Goodhue and Thompson [cf. TTF 1995].

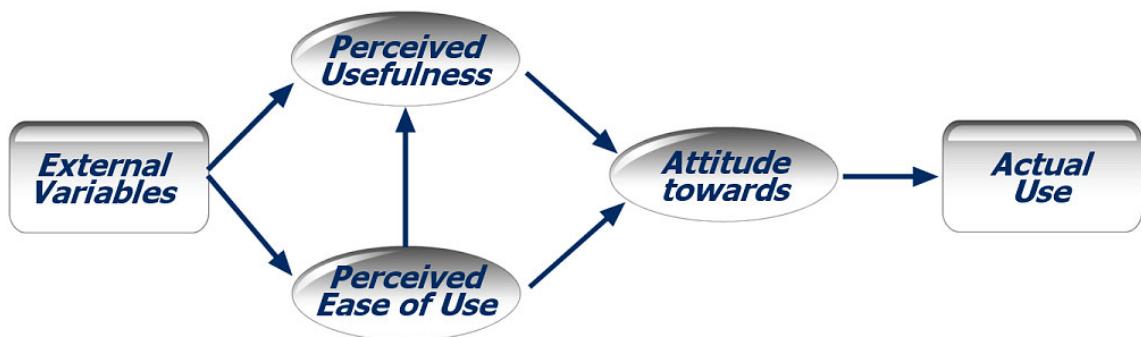


Figure 31: The TAM Theory

The TAM theory states that certain behaviour is determined by intention to perform the behaviour. The traditional TAM includes four concepts: ease of use, usefulness, attitudes towards use and intention to use. TAM identifies perceived ease of use, and perceived usefulness as key independent variables. Perceived usefulness is also indirectly influenced by perceived ease of use.

The TTF model addresses utilisation from a different perspective. The Task-Technology Fit is meant as the matching of the capabilities of the technology to the demands of the task. It posits that applications will be used only if the functions available to the user support / fit the activities of the user. Applications, which do not offer sufficient advantage, will not be used.<sup>130</sup>

Usability, as defined by the international ergonomics standard ISO 9241-10 refers to: "The effectiveness, efficiency, and satisfaction with which specified users achieve specified goals in particular environments." Here effectiveness is seen as "accuracy and completeness with which

<sup>130</sup> Cf. Dishaw/Strong/Bandy, [http://melody.syr.edu/hci/amcis02\\_minitrack/RIP/Dishaw.pdf](http://melody.syr.edu/hci/amcis02_minitrack/RIP/Dishaw.pdf).

specified users can achieve specified goals in particular environments", efficiency as "resources expended in relation to the accuracy and completeness of goals achieved" and satisfaction as "comfort and acceptability of the work system to its users and other people affected by its use" [cf. ISO9241 1996]. In another ISO standard, which focuses on software quality certain usability aspects such as documentation, ease of understanding, functionality, stability and reliability are explained [cf. ISO12119 1994]. The IEEE defines usability as "the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component" [cf. IEEE 1990].

"The abundance of information on the World Wide Web has thrilled some, but frightened others. Improved web site design may increase users' successful experiences and positive attitudes", writes Ben Shneiderman [cf. Shneiderman 1998]. His review of design issues identifies genres of web sites, goals of designers, communities of users, and a spectrum of tasks. An Objects/Actions Interface Model is offered as a way to think about designing and evaluating web sites. Finally, search and navigation improvements are described to bring consistency, comprehensibility, and user control.

It is essential that IMA can be used without prior knowledge of their internal workings. So from the user perspective usability is one of the most important requirements for appointing an IMA.

The user interface of an IMA must support the user in interpreting the context and situation and choosing a desired identity:

- Managing one's identities in the digital world is different from the intuitive behaviour in the off-line world where most communications are face-to-face and where aggregation of personal data and other information is a resource and time consuming task.
- The user interfaces should support various devices like home PCs, PDAs, mobile phones or in future even ubiquitous tokens and chips which vary in screen resolution, computing power, memory, input and output channels etc.
- The management of identities exists in the context of privacy and other regulation, which can be quite complex. Visualising the actors' rights and obligations is not trivial.

Not every action within the scope of an IMS is translated for the user via a graphical or other user interface. Conventionally many actions are performed implicitly.

Usability is typically more important for private users than professional organisations. Any enhancement of usability is more a question of affordability.

A lack of usability can have a negative impact on functionality, security and privacy.

### **2.2.3 Security**

An Identity Management System has to be as robust as possible against attacks on the availability, integrity and confidentiality of its services and information. This is particularly important because of the concentrated bulk of information about the user it stores and represents. There are risks of spying, manipulation and especially identity theft. If someone is using a foreign identity without authorisation, it could be difficult or impossible for the authorised person to prove that it wasn't him acting. Digital fraud may not be easily detectable for a contractual partner. The result will commonly be a liability risk for one party and a risk of loss of assets for the other.

Not only the total identity could be captured, but also the reputation linked to an identity. This kind of manipulation or unauthorised transfer of reputation is necessarily possible in the on-line world like, e.g., eBay allows its users to change the eBay name but continues the reputation

---

reviews. An IMS has to prevent reputation theft as well as prevent plagiarism and allowing non-repudiability if desired.

A basic requirement for security is that an authentication is needed before every kind of data access to assure that only authorised people have access. The form of authentication (like usage of biometrics) belongs to the kind of data and the performed action.

The type and grade of security required depends on the significance and value of the processed data. When only collecting information (such as browsing the web), security may not be so important as when a person administers his medical history. A consumer will typically be interested in protecting his accounting connection and, e.g., information about his credit card number. When citizens are interacting with the government to fulfil their civic duties (as in the case of tax declaration) or exerting their rights security is also an important factor. Because of the bulk of identity information stored and managed by organisations, security is an essential requirement for the service provider, too. Within the scope of their privacy policy organisations and particularly the government will be committed to do everything to keep their data in secure custody.

#### **2.2.4 Privacy**

Privacy is important in every scenario to be legal compliant. The Internet and all technical communication have to comply with laws and regulations concerning the respective (privacy) rights and privileges of the user and the provider. An IMA has to implement these rules as depicted below. While ultimately the user will be held accountable for his compliance with legal regulations, transactions performed within an IMS may be not at all transparent for him and prevent him from making an informed choice.

With respect to privacy regulation, this means for IMS:

IMA can fulfil privacy regulation and even the principles of Privacy-Enhancing Technologies. If the IMA is situated at the side of the user who has full control over his personal data and the way it is processed, it should support the user in asserting his rights – as far it is possible – online.

If the user's personal data is stored and managed at a provider, it has to follow the legal restrictions. This means that the provider is only authorised to process the user's data when and as far as the user has consented. Using them for others than the indicated purposes is inhibited. Furthermore the provider is not automatically legitimised to transmit personal data to external companies. In Europe this even applies when a company buys a provider and gets its data files.

This is different for the USA where this applies only for data of European citizens if the US data processing company accepted the "Safe Harbor Principles". These principles are created for the USA because of Art. 25 of the European Data Protection Directive, which allows data transmission from Europe to other nations only if these guarantee, a comparable degree of privacy protection. They include some of the main principles of the Data Protection Directive. Their acceptance is voluntary, but after acceptance any violation can be punished.

Furthermore data that the provider collects about the use of his services are personal data, too, when the usage and information about the identity of the user are linked together. According to national law it can be necessary for the provider to delete all data after the usage or billing (see above).

Even though the data seems not to be very valuable it can be important to protect it because of risk of profiling by organisations and linkability. When connecting different data, new data could be the result with additional content. So an IMA has to prevent uncontrolled profiling without allowance of the user. As far as possible, privacy requirements should be supported by or generally implemented in ICT. It will never be sufficient to solely rely on technologies in

protecting one's privacy; always organisational means will need to be applied, not to mention the regulatory and enforcement system in which ICT are embedded. Sometimes it is not only possible to implement privacy functionality, but technology might provide better ways for privacy, thus enhancing the state-of-the-art or even bringing forward the notion of privacy in society.

Privacy-Enhancing Technologies have been defined as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system" [cf. Borking/Raab 2001].

Related is the concept of multilateral security [cf. Rannenberg/Pfitzmann/Müller 1996; 1999]: Consider an action that involves communication between different parties. Multilateral security means providing security for all parties concerned in that communication. Multilateral security requires that each party only minimally trusts the others. The basic concept includes:

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

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

IMA can be built according the principles of Privacy-Enhancing Technologies, which can offer better privacy protection implemented into technology. These principles can be derived from today's privacy acts [cf. Hansen 2003] and are summarised in the sequel:

- Transparency:  
being aware of what personal data is transmitted/prompted and how it is processed;
- Data minimisation:  
reduction of processed personal data by anonymity and pseudonymity procedures, minimising the linkability between a person and the personal data [cf. Pfitzmann 1999];
- System integration:  
privacy protection built into the system;
- User empowering:  
privacy self-protection for users;
- Multilateral security:  
realisation so that only minimal trust in other parties is required.

The main concept for privacy-enhancing technologies is user-controlled linkability of one's personal data: Of course user control need transparency for informed choices, data minimisation for unlinkability procedures, system integration, empowering of the user to assert his privacy rights, and an environment which does not rely on blind trust [cf. Clauß/Pfitzmann/Hansen/Van Herreweghen 2002]. IMA where the user has full control over his personal data fulfil all these criteria and can be an example for Privacy-Enhancing Technologies. Obviously not all IMA are privacy-enhancing.

## 2.2.5 Law Enforcement

Law enforcement agencies are typically interested in collecting as much information as possible for giving evidence and make criminal proceedings easier and more effective.

---

A report issued by the US President's Working Group on Unlawful Conduct on the Internet presents the problems that law enforcement agencies have with strict encryption and data minimisation: "Encryption now presents and will continue to present a challenge to law enforcement confronting Internet-related crime. Robust encryption products make it difficult or impossible for law enforcement to collect usable evidence using traditional methods, such as court-authorised wiretaps and search warrants". And later: "U.S. law enforcement may be significantly affected by the 1995 and 1997 directives of the European Union ("EU") concerning the processing of personal data, including the deletion of traffic data. EU Member States are in the process of developing and implementing legislation. As the directives are implemented into national legislation throughout the EU, it is vital that public safety be considered, along with the privacy and market force elements."<sup>131</sup>

Enfopol, a council of the European Union, discusses law enforcement and operational needs with respect to public telecommunication networks and services as reported in a paper from March 2001.<sup>132</sup> The web site "State Watch" by Tony Bunyan, which monitors the state of civil liberties within the European Union, summarises this in the following way: "the demands of the law enforcement agencies centre on the issue of 'data retention', that is the recording and storage of all telecommunication data: every phone call, every mobile phone call, every fax, every e-mail, every web site's contents, all Internet usage, from anywhere, by everyone, to be recorded, archived and be accessible for at least seven years".<sup>133</sup>

This remains in stark contrast to the objectives and requirements of privacy protection and the legal requirement in some countries to delete needless personal data. Some countries have the basic principle that every notice, recording and using of (communication) data has to be legalised by an explicit law (e.g., cf. in Germany the G10 Law). In other legal systems like in the USA an obligation for developers to integrate access possibilities for law enforcement agencies in all applications is being discussed. This can lead to prohibition of cryptography if the user doesn't depose a decryption key at an official place. Also some politicians in Great Britain had and have this idea of key-escrow built<sup>134</sup>.

1993 the American administration made a proposal comparable with the key-escrow procedure. Their idea was a "Clipper-Chip", a chip build in every communication unit to give the administration a general key. But before readiness for marketing it was hacked.

In the aftermath of the 11<sup>th</sup> September 2001 terrorist attacks the senator of New Hampshire, Judd Gregg, called for a global prohibition on encryption products without backdoors for government surveillance.<sup>135</sup> The draft of a "Domestic Security Enhancement Act of 2003" by the US Justice Dept. heads for a comparable concept as it tries to prosecute the using of special cryptographic techniques.<sup>136</sup>

The Directive 2002/58/EG emphatically mentions the facility of data retention of communication services, which means the collection and saving of communication data for criminal prosecution.

Any IMS has to take care about the legal requirements for law enforcement of the countries where it should be used. As these requirements are sometimes contradictory, this is an exceedingly difficult subject.

---

<sup>131</sup> <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm>.

<sup>132</sup> <http://www.statewatch.org/news/2001/may/enfo7616.htm>.

<sup>133</sup> <http://www.statewatch.org/news/2001/may/03Benfopol.htm>.

<sup>134</sup> [http://news.bbc.co.uk/1/hi/uk\\_politics/1568254.stm](http://news.bbc.co.uk/1/hi/uk_politics/1568254.stm).

<sup>135</sup> <http://www.wired.com/news/politics/0,1283,46816,00.html>.

<sup>136</sup> Cf. <http://publicintegrity.org/dtaweb/report.asp?ReportID=502&L1=10&L2=10&L3=0&L4=0&L5=0>.

## 2.2.6 Trustworthiness

It is a prerequisite for all transactions that the user trusts the provider of a service or the IT system. Even in systems where the user has complete control over hardware, software and data flow [cf. Pfitzmann/Pfitzmann/Schunter/Waidner 1999], a certain amount of trust is still required because the complexity of the system defies transparency. Therefore, the reputation of software and hardware suppliers and IM service providers becomes an asset in the market. Although the notion of trust is irrational and may depend on many factors, it is clear that privacy, security and usability are preconditions for trustworthiness. Also possibilities for prosecution of claim and law enforcement influence the perception of trust.

## 2.2.7 Affordability

Every technology needs to be affordable to become widely accepted. This applies to all kinds of users but can be rephrased to the question if the IMS only adds overhead or enhances the functionality and/or quality of a given transaction.

It is a stated political goal in many countries that the right to informational self-determination is a basic right, and as such should not depend on the financial wealth of a person.

Organisations will look at IMS less from a cost but from a cost-effectiveness angle. In other words, the benefits of an IMS need to outweigh its direct (e.g., implementation) and indirect (e.g., process re-engineering) cost.

## 2.2.8 Interoperability

Compatibility and integration with existing systems are basic requirements for an IMA. The IMA should implement interfaces compatible with international standards. In order to achieve sufficient market penetration, these interfaces should be accepted and supported by the dominant players in the respective markets for IMA.

These stakeholders will legitimately seek to influence any standard in order to support it. It is entirely possible that certain players will resist compatible interfaces in order to protect their market position. In such a case, the acquisition of critical mass for IMA as a product may be more difficult. Trust regulations may be able to regulate isolationist tendencies in the market.

## 2.3 Mechanisms

In the preceding Chapters basic requirements to IMS were elaborated. This Chapter analyses the mechanisms, i.e., measures which can be taken to meet these requirements, taken from relevant literature.

The mechanisms described in this Chapter have been developed predominantly from a technology perspective; in fact they are mechanisms for IMA rather than for full IMS. The following table illustrates this by giving an overview of mechanisms for IMS and their maturity, meaning whether they are

- Widely *distributed* in practice;
- *Available*, but not widely distributed;
- Have *prototype* character;
- Are worked out on a *conceptual* level;
- Are only mentioned as an *idea* or
- Are pure *visions* until now.

**Table 18: IMS Mechanisms with Respect to Requirements**

<b>Requirement</b>	<b>Mechanisms</b>	<b>Maturity</b>
Functionality: Identity Administration	<p><b>Communication-independent handling and representation of identities:</b></p> <ul style="list-style-type: none"> <li>- Using existing data management systems and data schemes</li> <li>- Creating, updating, deleting identities and identity information</li> <li>- Integrating authentication data, esp. for single sign-on</li> <li>- Integrating certificates and signatures</li> </ul> <p><b>Pseudonyms with specific properties</b></p> <p><b>Credentials</b></p> <p><b>Identity recovery</b></p> <p><b>Interfaces:</b></p> <ul style="list-style-type: none"> <li>- Communication interface</li> <li>- Import and export interfaces</li> </ul> <p><b>History management:</b></p> <ul style="list-style-type: none"> <li>- Logging transactions</li> <li>- Representing transaction history/context information</li> <li>- Illustrating what the communication partner knows from previous transactions</li> <li>- Analysing log files</li> </ul> <p><b>Privacy control functionality:</b></p> <ul style="list-style-type: none"> <li>- Consent, objection, disclosure, correction, deletion</li> <li>- Integration of additional privacy information on the application</li> </ul> <p><b>Context detection</b></p>	Distributed Distributed Available Available Concept/idea Prototype Available Available Available
Functionality: Gateway		
Functionality: Notice		
Functionality: Control	<p><b>Rule handling:</b></p> <ul style="list-style-type: none"> <li>- Reasonable and privacy-friendly default settings</li> <li>- Configuring preferences, e.g., when to transmit which data, which degree of anonymity/accountability</li> </ul> <p><b>Handling of identities in the communication:</b></p> <ul style="list-style-type: none"> <li>- Choice among different identities</li> <li>- Negotiation</li> <li>- Single Sign-On</li> <li>- Automatic fill-in</li> </ul> <p><b>Environment requirements:</b></p> <ul style="list-style-type: none"> <li>- Anonymous communication network</li> <li>- Secure systems</li> </ul>	Available for specific applications; vision for general solutions Concept Concept
Usability	<ul style="list-style-type: none"> <li>- Comfortable and informative user interfaces</li> <li>- Raising awareness</li> <li>- Training and education</li> <li>- Reduction of legal/technology/... system's complexity</li> <li>- Simulating common situations</li> </ul>	Concept; vision for general solutions Idea Available Idea Concept
Security	<ul style="list-style-type: none"> <li>- Mechanisms for confidentiality, e.g., secrecy, anonymity</li> <li>- Mechanisms for integrity incl. accountability</li> <li>- Mechanisms for availability</li> <li>- Fallback solutions (redundancy, fragmentation,</li> </ul>	Available Available Available Available

	keeping "old-world processes")	
Privacy	<ul style="list-style-type: none"> <li>- Data minimisation</li> <li>- P3P</li> <li>- Privacy seals</li> <li>- Penalties</li> </ul>	Prototype Available Available Available
Law Enforcement / Liability	<ul style="list-style-type: none"> <li>- Digital evidence</li> <li>- Digital signatures</li> <li>- History functions</li> <li>- Data retention</li> </ul>	Concept Available Available Prototype
Trustworthiness	<ul style="list-style-type: none"> <li>- Segregation of power, separating knowledge, integrating independent parties, e.g., as operators or providers</li> <li>- Open Source</li> <li>- Trusted seals of approval</li> </ul>	Available  Available Prototype
Affordability	<ul style="list-style-type: none"> <li>- Powers of market</li> <li>- (State) subsidies for development, use, operation, etc.</li> <li>- Using open source building blocks</li> </ul>	Concept Concept Available
Interoperability	<ul style="list-style-type: none"> <li>- Compliance to existing (de facto-) standards</li> <li>- Setting (open) standards</li> </ul>	Concept Idea

In the following Chapters we will concentrate on mechanisms for IMA. Although different kinds of IMA exist, their common denominator with respect to mechanisms is "the user's management of identity data". According to the IMA's respective functionalities additional mechanisms may be of interest. Because this study focuses on multi-purpose IMS, those specific mechanisms are not presented in detail. Instead, we describe mechanisms according to the functionality requirements (cf. Chapter 2.2.1), complemented by mechanisms for privacy-enhancing IMA components which give main attention to user-controlled linkability.

### 2.3.1 Communication-Independent Handling and Representation of Identities

In terms of technology, management of identities means provision of mechanisms for identity administration through their lifecycle. The components of such a partial identity may vary according to applications or contexts, but typically the following components can be found in a data set of a partial identity:

- Identifier: a pseudonym (cf. Chapter 2.3.2) which acts as a unique ID (unique in the specific context, not necessarily globally unique) and may also function as an address;
- Data: like address, interests, etc.;
- Certificates.

The user should have the possibility to create his partial identities, update identity data and delete identity data and partial identities.<sup>137</sup> The administration of identities should not only cover one's own partial identities, but may be extended to those of his communication partners as far as they are stored within one's own IMA. The data attributes of a partial identity may be a fixed set which can be filled in (or left blank) by the user, or the data set may be configured, e.g., by the user or the application.

Additionally the user should be able to handle digital signatures of his partial identities (e.g., signing) and of partial identities of transaction parties (esp. checking digital signatures).

---

<sup>137</sup> Similar [OpenGroup 2002]: "Create identity, update identity information, destroy identity, archive identity information, obtain identity information, present identity, verify identity, signature, apply information access control for update and read-access, create and maintain identity information stores, synchronise identity information stores, split and merge stores to reflect organisational changes".

---

In principle any means of digital storage and addressing the stored data can be used, e.g., semiconductor RAM, hard- or floppy disks or any other media.<sup>138</sup> All the same, data management systems like databases or file systems can be used.

Some standardised data schemes for managing personal data have been proposed, e.g., within W3C's P3P ("Platform for Privacy Preferences")<sup>139</sup> or CPEX ("Global standards for privacy-enabled customer data exchange")<sup>140</sup>.

The handling of identities can be performed by any kind of computers, e.g., servers in the Internet, desktop computers at home or at the office, notebooks, which can be used in "nomadic environments" as well, PDAs, mobile phones [e.g., cf. Fischer-Hübner/Nilsson/Lindskog 2002; Nilsson/Lindskog/Fischer-Hübner 2001], chip cards or tokens being used in ubiquitous computing. Of course differences in available resources or in trust areas have to be taken into account when implementing this functionality.

The type of device the IMA is implemented in determines the possibility for representing partial identities to the user. In some cases identity management can be a seamless process, using reasonable default settings. In some cases the user has to be actively informed or asked for decision by the IMA – then identity management becomes explicit. It is explicit, too, as far as the user configures his partial identities and preferences, a process similar to setting up an address book and keeping it up-to-date. For users who do not want to invest time in such procedures, learning modes can be offered, e.g., similar to PC firewalls or even self-learning methods, interpreting the user behaviour.

The usability aspect is of utmost importance [cf. Jendricke/Gerd tom Markotten 2000]. Concepts for simulating common situations the user can grasp immediately are being discussed, e.g., in [cf. Hansen/Berlich 2003], taking up the idea of Virtual Residence [cf. Beslay/Punie 2002].

Handling and representation of identities are the basis for an informed choice (cf. Chapter 2.2.1).

### **2.3.2 Pseudonyms with Specific Properties**

User-controlled linkability is the core concept of real identity management. This means that the IMS has to realise unlinkability of different actions of a user so that communication partners involved in different actions of the same user cannot aggregate the personal data disseminated during these actions for user profiling. This is even possible with authenticated data when specific pseudonyms are used [cf. Chaum 1985; Pfitzmann/Waidner/Pfitzmann 1990/2000].

Pseudonymity comprises all degrees of linkability to a person – including anonymity and accountability. Reputation may be established or consolidated by using the same pseudonym. IMS providers possibly dealing with pseudonyms have already been introduced in Chapter 1.5.2.

---

<sup>138</sup> From the privacy point of view media without the option for secure data erasure are undesirable.

<sup>139</sup> <http://www.w3.org/P3P/>.

<sup>140</sup> <http://www.cpeexchange.org/>.

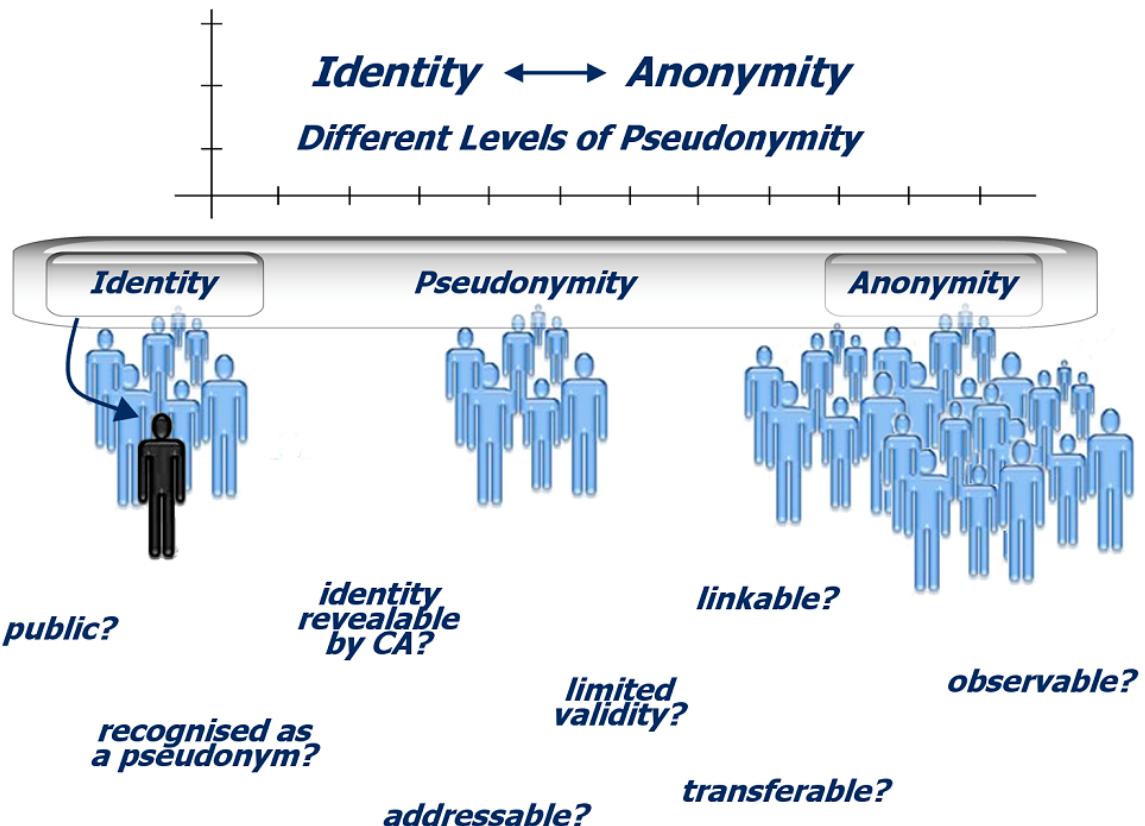


Figure 32: Pseudonymity as the Full Range between Identity and Anonymity<sup>141</sup>

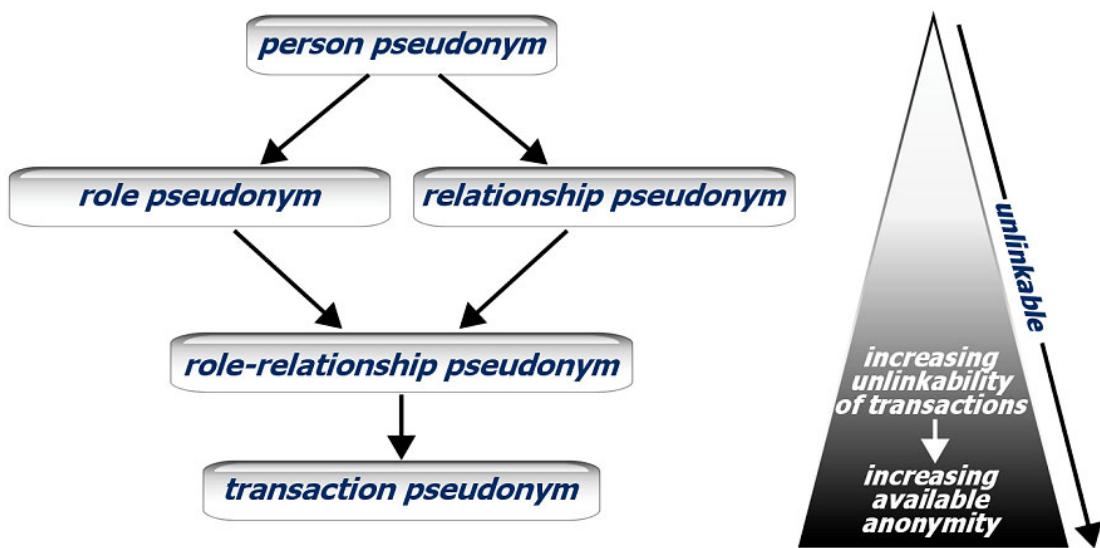
A pseudonym together with the data linked to it forms a partial identity. Relevant important properties of pseudonyms include [cf. Clauß/Köhntopp 2001]:

- Authentication and authorisation:  
Credentials or attribute certificates bound to digital pseudonyms support authentication and authorisation. For authorisation purposes, it is possible to use transferable digital vouchers, which could be implemented by blind digital signatures or certificates.
- Initial knowledge of holdership [cf. Roßnagel/Scholz 2000]:  
Pseudonyms can be generated by the user or generated and assigned by a third party, e.g., an application provider. In the context of identity management, the linkage between a pseudonym and its holder would not be publicly known by default.
- Proof of holdership:  
Proof of holdership is the capability to prove ownership to a pseudonym without disclosing additional personal information. *Digital pseudonyms* could be realised as a public key to test digital signatures where the holder of the pseudonym can prove holdership by forming a digital signature, which is created using the corresponding private key [cf. Chaum 1981]. For instance, PGP public keys, which are bound to e-mail addresses, are digital pseudonyms.
- Cross-contextual linkability:  
If the same pseudonym is used many times or in different contexts, the corresponding data about the holder, disclosed in any of these events, can be linked. In general, anonymity is the stronger, the less often and the less context-spanning the same pseudonyms are used. We distinguish *transaction pseudonyms*, which are only used for a single transaction, a group of situational pseudonyms, which are used in a specific context (e.g., according to the *role* of the holder or the *relationship* to the communication partner), and context-spanning

<sup>141</sup> [Köhntopp 1999; Pfitzmann/Köhntopp 2001].

*person pseudonyms* as substitutes for the holder's name respectively civil identity (cf. Figure 33).

- Convertibility (transferability of attributes of one pseudonym to another):  
In an anonymous credential system as introduced by David Chaum [Chaum 1985] users are known to different organisations by different pseudonyms (cf. Chapter 2.3.3). Different pseudonyms of the same user cannot be linked. Yet, an organisation can issue a credential (attribute certificate) to a pseudonym, and the corresponding user can prove possession of this credential to another organisation (who knows him or her by a different pseudonym), without revealing anything more than the fact that she owns such a credential. Possession of a credential can be demonstrated repeatedly under different pseudonyms without these pseudonyms becoming linkable. Nevertheless, proving possession of several credentials obtained under different pseudonyms is only possible when these credentials were indeed issued to the same user, i.e., different users cannot pool their credentials.



**Figure 33: Pseudonyms With Different Degrees of Cross-Contextual Linkability**

There are several other properties of pseudonyms within the system of their use, which shall only be shortly mentioned. They comprise different degrees of, e.g.:

- Limitation to a fixed number of pseudonyms per subject [cf. Chaum 1981, 1985, 1990],
- Guaranteed uniqueness [cf. Chaum 1981, Stubblebine/Syverson 2000],
- Transferability to other subjects,
- Authenticity of the linking between a pseudonym and its holder (possibilities of verification/falsification or indication/repudiation),
- Possibility and frequency of pseudonym changeover,
- Limitation in number of uses,
- Validity (e.g., time limit, restriction to a specific application),
- Possibility of revocation or blocking, or
- Participation of users or other parties in forming the pseudonyms.

In addition, there may be some properties for specific applications (e.g., addressable pseudonyms serve as a communication address) or due to the participation of third parties (e.g., in order to circulate the pseudonyms, to reveal identities in case of abuse, or to cover claims).

Some of the properties can easily be implemented by extending a digital pseudonym by attributes of some kind, e.g., a communication address, and specifying the appropriate

semantics. The binding of attributes to a pseudonym can be documented in an attribute certificate produced either by the holder himself or by a certification authority.

IMS can support all these kinds of pseudonyms. To be considered privacy-enhancing, an IMS needs to allow the user to choose his required and acceptable degree of pseudonymity while maintaining the conventional capabilities for identification, authentication, authorisation, and non-repudiation.

Depending on the situation, different properties are needed. A privacy-enhancing IMS should be flexible in adaptation of properties to situations. For maximising privacy, the default setting for privacy-enhancing IMS should be transaction pseudonyms respectively role-relationship pseudonyms where linkability in the specific context is desired. The privacy-enhancing IMS should support anonymous credentials.

### 2.3.3 Credentials

Technological solutions like the digital signatures for enabling accountability of communication partners and their transactions lead to a privacy threat because all transactions under the same signature could be linked, composing an informative profile of an individual. With both accountability and privacy, credentials meet two main requirements for IMS: Although an authorisations is bound to an individual and can be reliably used in many contexts, its use does not lead to data trails or unwanted disclosure of personal data. As long as the individual does not misuse the credential, anonymity is guaranteed.

In more detail: The individual can obtain a convertible *credential* from one organisation using one of her pseudonyms, but can demonstrate possession of the credential to another organisation without revealing her first pseudonym. For this purpose, a credential can be converted into a credential for the currently used pseudonym. Therefore the use of different credentials is unlinkable. Chaum published the first credential system by [cf. Chaum 1985]. Other systems have been proposed.<sup>142</sup> The integration of credentials in an IMS infrastructure is shown in Figure 34.

---

<sup>142</sup> [Cf. Chaum/Evertse 1987; Damgaard 1990; Chen 1995; Brands 1999; Lysyanskaya/Rivest/Sahai/Wolf 1999; Camenisch/Lysyanskaya 2001].

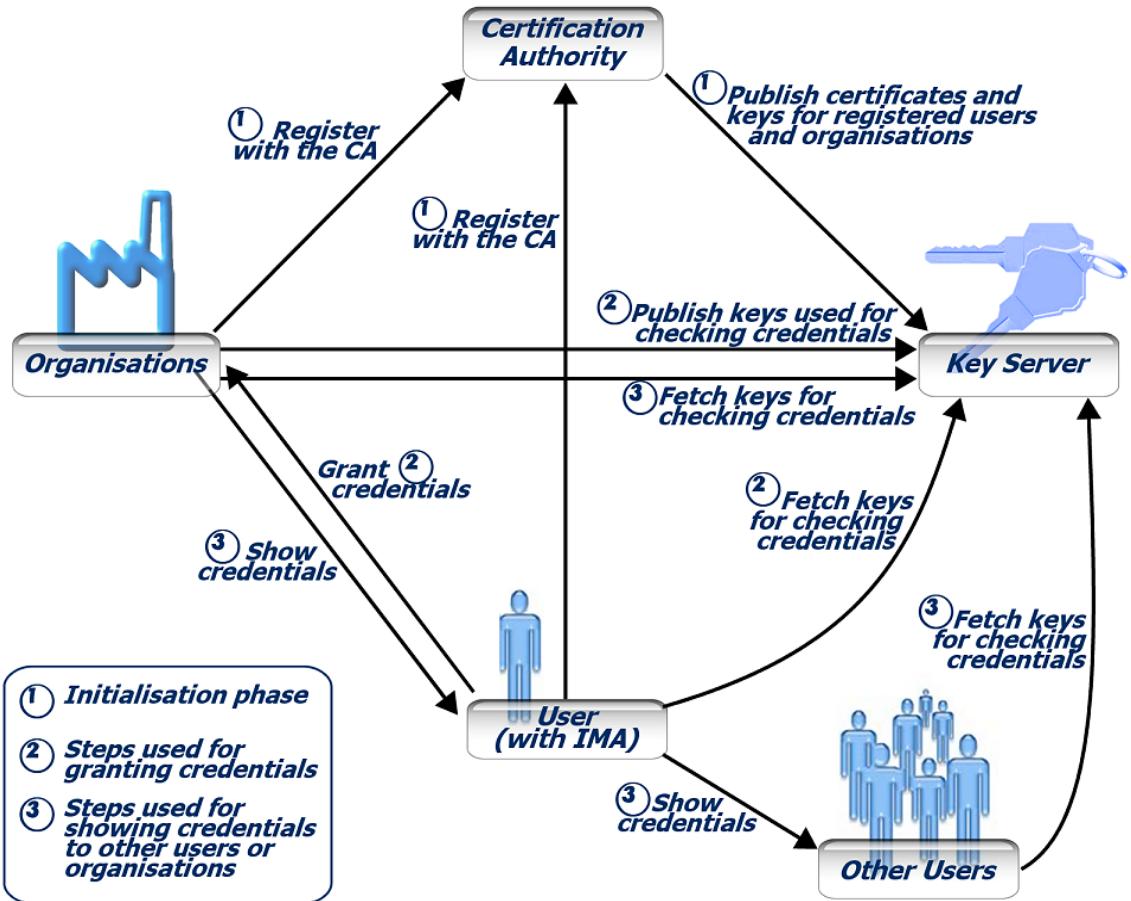


Figure 34: Data Flow Concerning Credentials in an IMS

For instance, if a service can only be used by authorised users, but the individuals want to remain anonymous to the service, they need to show authorisations (i.e., credentials) to the service which are issued by a third party and which are unlinkable to their pseudonyms.

By issuing a credential, an organisation certifies that the user owns a specific property or right. For instance, a governmental institution, such as a registration office, may issue credentials on the user's identification data like the name or the date of birth. One could also imagine credentials on the driving licence, age or rights of vote. A bank could certify that a user disposes of a specific amount of money. Credit notes could also be issued by means of credentials.

When a user gets a credential, he or she can link it on demand to a pseudonym used during an action. The communication partner receiving the pseudonym verifies the credentials to get the information certified by the credential issuing organisations. In order to verify a credential some information of the credential issuing organisation is needed, e.g., keys obtained from a PKI. These keys must be certified by the organisations and published on key servers, so that each potential verifier has access to them.

Figure 34 shows the entities needed when working with credentials, namely:

- Certification authorities where organisations and users can obtain certificates from;
- Key servers where all published (certified) keys can be fetched from, especially the keys used to verify credentials;
- Organisations which issue credentials to the users and publish keys to verify these credentials.

### 2.3.4 Identity Recovery

In some cases it might be necessary to recover used identities. The user may rely on a backup solution preventing great data loss after a malfunction or crash of the IMA. On the other hand, other parties may have legitimate interest in recovering used identities, e.g., in the case of misuse or fraud. Where such identity recovery functionality is desired or required, such information on identities could be stored at identity brokers<sup>143</sup> which may disclose these data under predefined conditions. The principle of separation of knowledge should apply in those cases.

### 2.3.5 Interfaces for Communication and Import/Export

The IMA can only control and monitor communication where it is integrated, e.g., as a gateway to a digital network. Thus, a comprehensive multi-purpose IMA should be able to interface with various applications and devices. As an IMA is only capable of supporting the user as far as it handles the personal data and communication, there are natural boundaries to the individual's life in the real world and outbound data collection, e.g., by biometric surveillance (cf. Chapter 1.2.3).

Interfaces may not only exist on the communication level, but also considering the configuration of the IMA itself, e.g., for exchanging configuration files or semantic relevant information on data processing procedures by organisations. Users may prefer importing preference configurations or rules from other sources rather than the vendor or organisation, e.g., from other users with similar interests or third parties, which may provide specific, e.g., privacy-checked files. A privacy information service may help by offering additional information on potential privacy risks (e.g., like a PERT – Privacy Emergency Response Team [cf. Clauß/Köhntopp 2001]) or provide other information on the context.

If users desire to export their files, e.g., for other devices or for other interested users, an output interface should be supported.

### 2.3.6 History Management

To enable a user's record keeping of the dissemination of personal data, the IMA logs the data released and is capable of representing release history and context information to the user in a concise but meaningful way. This helps to illustrate how much the communication partner knows about oneself from previous transactions. History information includes the extent, nature, and linkability of data released in the past. Additional information may be used when analysing the log file, e.g., on the trustworthiness of the communication partner, on current privacy or security risks etc. Of course this way of "data mining" is less powerful than the aggregation and data mining procedures of larger organisations with access to bigger quantities of data. But it does provide more transparency and support user awareness.

The handling of such logs and their interpretation is related to certain topics of current interest: How to obtain an accurate estimation of a potential privacy risk out of a log file? How to avoid generating "data cemeteries" – with all their implications for storage and retrieval overhead and uncontrolled storage of personal data? What is more, when logging personal data of communication partners, their data is stored as well. This means that the user will himself be considered a data processing party so that data protection and other legal regulations apply.

### 2.3.7 Privacy Control Functionality

Privacy control functionality like in DASIT<sup>144</sup> [cf. Enzmann/Schulze 2001] can supplement the Identity Management System by giving each user information about his personal data stored at a

<sup>143</sup> Outside the user's IMA.

<sup>144</sup> Datenschutz in Telediensten (Privacy Protection in the Internet by User Control).

---

server, allowing him access to these data, and give him the means to correct these data, to remove them, or to grant or revoke consent. This functionality implements legal privacy rights of European citizens by overcoming the inhibition of having to change back to off-line world to assert one's rights. A direct access to the server's databases of course normally requires modifications in their software and should not impact the security level previously achieved.

Adding structured information on data processing policies of the organisation (e.g., P3P) or on the handling of transactions (e.g., by specific tags added in the transfer protocols) can support the system's transparency and the user's awareness.

### **2.3.8     Context Detection**

Context information may include additional information, e.g., specific tags to express when actions have to be linked or what properties a new pseudonym should have. They could be provided by communication partners, third parties such as a privacy information service or even the Internet community [cf. Hansen/Berlich 2003].

Automatic context detection to help the user in managing his or her identities<sup>145</sup> may be added to the communication protocol (integrated in an Identity Management Protocol Set (cf. Chapter 1.3.1)). The latter would have to be standardised to be effective and should not only describe the context, but requirements or degrees of freedom concerning pseudonym properties as well.

### **2.3.9     Rule Handling**

Managing one's identity should not lead to an endless prompting of the user to manually decide on the use of partial identities in each part of a transaction. Instead there should be a technical support where the user uses preferences with rules for when and under what conditions to re-use pseudonyms and when new ones should be created or obtained, being interpreted solely by the client or matched against server policies [cf. Cranor 1999]. Context detection should be supported by an appropriate rule handling to enable an automatic choice.

In all cases reasonable and privacy-friendly default settings, e.g., unlinkability (i.e., transaction pseudonyms) as a default in unknown contexts should be applied.

### **2.3.10    Handling of Identities in the Communication**

The user should have the possibility of making an informed choice of his identities and related data. Besides context detection and rule handling, the following mechanisms are capable of supporting him:

- Offering different partial identities if appropriate while showing their specific properties;
- Helping the user with Single Sign-On processes and automatic fill-in form procedures according to his preferences;
- Support of negotiation on the circumstances of data transmission [e.g., cf. Damker/Pordeschn/Reichenbach 1999; Koch/Wörndl 2001].

### **2.3.11    Infrastructural Environment Requirements: Anonymous Communication Network and Secure Systems**

A prerequisite for achieving unlinkability of actions at the application level is support of anonymity by the network, e.g., realised with Mix-based anonymity services [cf. Chaum 1981; Berthold/Federrath/Köhntopp 2000; Bäumler/von Mutius 2003].

---

<sup>145</sup> E.g., by interpretation of hints which are related to known contexts or situations or by interpretation of specific tags to express when actions have to be linked or what properties a new pseudonym should have.

If users act under pseudonyms, service providers can enforce security and authenticity only if they accept pseudonymous or anonymous credentials. Misuse may be prevented (instead of only being traced) by integrating appropriate security mechanisms into an application.

An IMA stores and processes sensitive personal data. Therefore, IMA and its communication should ensure a high security level, by technological and organisational measures.<sup>146</sup> The user's control over his IMA could be achieved by implementing the identity management functionality in trustworthy hardware, e.g., in small PDAs.

### **2.3.12 Mechanisms for Trustworthiness**

#### **2.3.12.1 Segregation of Power**

Appropriate segregation of power is a prerequisite for trust. Parties in any transaction will only command limited trust on part of their business partner. Segregation should be vertical (along process steps) and horizontal (with no single party being able to monopolise or bottleneck the process). The market, in which trusted third parties offer their services needs to be sufficiently mature, so that the user can choose a supplier based on their performance. No single competitor would then easily achieve a dominating position with the potential for abuse of power.

Different parties can participate in such a market, such as enterprises, independent institutions (such as privacy protection authorities), interest groups or an appropriately organised bulk of users (as is the case with credentials for digital signatures in a PGP web of trust).

#### **2.3.12.2 Openness / Open Source**

An open process for development of IT systems and the disclosure of source code can increase trustworthiness. Certain security and privacy goals cannot be validated by practical experience, e.g., confidentiality, which requires that information won't leak out. Those properties can only be validated by disclosure of sources. Of course a formal proof is impossible without the most detailed information on the IT system including the source code. Furthermore, as has been proven in a large number of open source projects, an open and co-operative software development can lead to robust and reliable products. Nevertheless, this is no automatism, but requires adequate diligence during the entire development process and during the evaluation by experts [cf. Hansen/Köhntopp/Pfitzmann 2002].

#### **2.3.12.3 Seal of Approval**

Complex IT systems are not easily controlled with regard to their security, safety and privacy. Privacy Seals, being a grade for trustworthiness, should certify that IT products or services at least apply to privacy protection law (being privacy-compliant) or are even privacy-enhancing. These days a variety of such privacy seals, mostly for specific application contexts like web sites, are available. Certain seals have a broad approach, as they strive to translate existing privacy regulation into evaluation criteria for IT systems. Others are more marketing-driven.

One well-known seal is the legally based "IT Seal of Quality"<sup>147</sup> from the Independent Centre for Privacy Protection (ICPP) Schleswig-Holstein, Germany [cf. Hansen/Probst 2002]. The privacy protection law of this state includes an obligation for public authorities to prefer the purchase and use of products which legal compliance to privacy protection law has been evaluated and stated. A similar regulation is found in other privacy protection laws as well, but only Schleswig-Holstein has thereby set up a system for evaluating the privacy compliance of IT systems until now.

---

<sup>146</sup> A detailed description of these measures, e.g., encryption, access control, biometrics, preventing theft of IMA, etc. is outside the scope of this study.

<sup>147</sup> <http://www.datenschutzzentrum.de/guetesiegel/>.

---

### 2.3.13 IMS Mechanisms with Respect to Co-operating Parties

As already stated in Chapter 1.4, functionality and performance of an IMS is highly dependent on which parties co-operate in the system. We introduce the following terms according to the type of the co-operating parties (similar in [Clauß/Köhntopp 2001]):

- If the user is left to his own devices, only *user-side technologies*<sup>148</sup> work.
- *Communication-partners technologies*<sup>149</sup> function only if the communication partners co-operate. This means that some co-ordination and negotiation is needed concerning their usage.
- *Third-parties technologies*<sup>150</sup> need a third party involvement to fulfil a specific task for other participating parties. This means that more co-ordination and negotiation is needed concerning their usage compared to user-side – and in most cases as well communication-partners – technologies.
- *Distributed technologies*<sup>151</sup> require many independent parties to co-operate. This means that co-ordination and negotiations must function on a large scale.

Table 19 restructures the mechanisms from Table 18, which are mainly technology-based, according to these terms and refines them for this purpose. This structured overview shows that many mechanisms of a comprehensive IMS can only be realised if other parties or the infrastructure support them [cf. Köhntopp 2001; Köhntopp/Pfitzmann 2001]. IMA, which offer, e.g., only user-side technologies, are limited in the extent and reliability of identity management functionality:

---

<sup>148</sup> Also called "unilateral technologies" [cf. Pfitzmann 2001b].

<sup>149</sup> Also called "bilateral technologies" [cf. Pfitzmann 2001b].

<sup>150</sup> Similar to "trilateral technologies" [cf. Pfitzmann 2001b].

<sup>151</sup> Similar to "multilateral technologies" [cf. Pfitzmann 2001b].

**Table 19: Technology-based IMS Mechanisms with Respect to Co-operating Parties**

Type of Co-operating Parties	Mechanism Concerning Identity Management
Single user	<p>Handling and administration of identities</p> <p>Generation of (digital) pseudonyms</p> <p>Binding of self-certified attributes to pseudonyms (self-authentication [cf. Chapter 1.1.3])</p> <p>Support user in choosing his identities</p> <p>Simple history management and rule handling:</p> <ul style="list-style-type: none"> <li>- Logging of data transmissions, structured (e.g., profiles) as well as unstructured (e.g., arbitrary text)</li> <li>- Interpretation of log files</li> <li>- Depiction of knowledge communication partners may have collected (based on logged data transmissions and additional information where applicable, e.g., linking with public databases or in case of known privacy violations), especially regarding linkability of various pseudonyms of a user</li> </ul> <p>Unilateral mechanisms such as trustworthy hardware [cf. Pfitzmann/Pfitzmann/Schunter/Waidner 1999], file/database encryption, strong authentication, user interfaces to negotiate protection goals, and configuration of what data may be transmitted under what condition (as far as unilaterally interpretable) [cf. Wolf/Pfitzmann 2000]</p>
Communication partners	<p>Issue and verification of certificates and credentials to be bound to pseudonyms [cf. Pfitzmann/Waidner/Pfitzmann 1990/2000]</p> <p>Issue of digital vouchers and customer account cards</p> <p>Simple context management, e.g., by tagging of start and end of transactions where linkability is required respectively announcement of context changes by the particular communication partner</p> <p>Privacy control functionality for users (consent, objection, disclosure, correction, deletion)</p> <p>Bilateral security mechanisms such as encryption of communication as well as configuration and, where applicable, negotiation of what data may be transmitted under what condition (as far as bilaterally interpretable)</p>
Integration of third parties	<p>Issue and verification of certificates and credentials</p> <p>Various types of trustees (identity brokers (also for identity recovery), value brokers, liability services) with integration into applications</p> <p>Authentication of attribute certificates or authorisations (e.g., ballot card, driving licence, identity card, passport) in form of credentials by public authorities or organisations</p> <p>Integration of privacy-enhancing payment services</p> <p>Integration of privacy-enhancing delivery services</p> <p>Providing configuration files conforming to or enhancing privacy (rules, additional context information) for communication partners by privacy information services</p> <p>Trilateral security mechanisms such as digital signatures as well as configuration of and, where applicable, negotiation of what data may be transmitted under which condition (as far as trilaterally interpretable)</p>
Distributed realisation with co-operation of many parties	<p>Separation of knowledge about identity data or linkability among multiple trustees</p> <p>Integration of a redundancy against denial of service attacks</p> <p>Utilisation of a "web of trust" for authentication purposes</p> <p>Utilisation of group pseudonyms</p> <p>Multilateral security mechanisms such as realisation of strong anonymity and unobservability</p>

---

We clearly see that the possible functionality of a pure unilateral identity management is quite restricted. For full functionality the communication partners have to support the IMS, third party services have to be integrated, and specific distributed mechanisms are required as well.

## 2.4 Summary

In this Chapter, general demands to be made on IMA/IMS have been worked out. For this purpose, typical scenarios have been developed and introduced according to which the meaning of these demands was pointed out in detail. The scenarios were: General Identity-related Scenarios with Identity Theft and Data Trails, General Scenario with Identity Protector, E-Shopping, E-Auction, E-Banking, Tax Declaration, Inquiry, E-Court with Civil Action, On-line Mediation and Criminal Proceedings, E-Voting, E-Health, E-Science, E-Notary and at last some notes about location based services. The following main requirements turned out to be stable: functionality, usability, security, privacy, law enforcement, trustworthiness, affordability and interoperability.

A first important result from the overall view of the scenarios and requirements consists in the fact that particular parts within an overall workflow are de-coupling from each others and can be composed to pseudonym domains. As far as different pseudonym domains exist, an IMS has to allow or support a pseudonym switch even within a workflow.

By use of the general requirements, the mechanisms for the technical realisation were derived. A second noticeable result from the overall view of these mechanisms consists in the necessity to consider the state of maturity a technology or a concept or an idea has reached in connection with identity management. For example, the question arises if a mechanism is given as... widely *distributed* in practise, *available* but not widely distributed, working as a *prototype*, worked out as an academic *concept* or mentioned as an *idea* or just a *vision*?

As outstanding mechanisms for the handling or the representation of identities, the different types of pseudonyms and credentials play a particular role. Credentials are convertible certifications by which authorisations a user has obtained by use of a pseudonym can be transferred to his other pseudonyms without being transferred to other users' pseudonyms. By use of these two mechanisms, the core concept of the "user-controlled, technology-based identity management" can be realised technologically. The requirements and mechanisms form the basis for the evaluation of existing IMA in the next Chapters.

### 3 [CHAPTER C: LIST OF EXISTING SYSTEMS]

This Chapter contains two lists of existing IMA from both academia and industry. The first is ordered by availability (concept, prototype, suspended prototype, and available), the second list is in alphabetic order. The listed IMA were collected by exploitation of

- Internet web sites, especially by top results in common search engines such as Google.com,
- exhibitions such as CeBIT,
- publications on IMS, e.g., in proceedings of specific workshops on security, privacy, usability, e-commerce, economy, and jurisdiction<sup>152</sup>,
- statements of the surveyed experts<sup>153</sup>.

For each IMA additional information is given as described in the following paragraphs. The notation is:

"Y": means that this criterion is completely fulfilled

"(Y)": means that this criterion is partly fulfilled

"N": means that the criterion is not fulfilled at all

"-": means that no declaration for this criterion is possible

"?": means that the degree of fulfilment is unknown

#### 3.1 Criteria

The criteria are divided in three parts. The "Basics" describe the basic information on the IMA like name, manufacturer and nation. The "Operational Areas" classify the IMA considering their primary use. The operational areas are combinations of different functionalities and mechanisms presented in Chapter 2 before. After collecting information about the existing IMA, it has been realised that these five operational areas characterise the different developments. Each IMA achieves at least one of the areas. At last the "Miscellaneous" part describes the status, basic characteristics of the system environment and specific notes.

##### 3.1.1 Basics

**Table 20: Basic Criteria**

Criteria	Description
Name	Name of the IMA
Manufacturer	Main manufacturer or provider of the IMA
Nation	Nation of the manufacturer's respectively provider's location

##### 3.1.2 Operational Areas

*Access Management (Authentication, Single Sign-On):* The IMA supports access management (AAA: authentication, authorisation, accounting) or enables the user, having logged on once per session, to access sites and services of different suppliers. Additionally digital signatures are handled in this category.

*Form Filling:* The IMA supports the user when filling in electronic forms (e.g., questionnaires at the registration to web sites) by filling in automatically or suggesting input values.<sup>154</sup>

<sup>152</sup> Except for publications on identity management in organisations like the Identity Management Initiative by SIMC (<http://www.simc-inc.org/identity>), which is not in the focus of this study and is therefore not incorporated into this list.

<sup>153</sup> Also pure anonymity tools were mentioned by the experts but they are not IMA according to the definition of this study. So they were not incorporated into this list.

<sup>154</sup> This implies in general the storage of personal data, a support in case of disclosure and a log function.

---

*Automatic Choice of Identity:* The IMA proposes the pseudonym appropriate for the current context. The user could describe how his or her personal data should be used by the communication partner or others (definition and matching of preferences and policies, e.g., by P3P and APPEL). Or the IMA could recognise, e.g., the situation of an on-line purchase and could apply appropriate (default) settings or give the user recommendations.

*Pseudonym Management:* The IMA supports different pseudonyms. This normally includes that the user has the possibility of choosing between different pseudonyms (at least two).

*Reachability Management:* The IMA puts users in a better position to handle their contacts by providing an intelligent filter mechanism, e.g., to prevent spam e-mail or unsolicited phone calls.

**Table 21: Criteria Operational Areas**

<b>Criteria</b>	<b>Description</b>
Access Management	Ensures authenticity (like single sign-on; use of digital signatures)
Form Filling	Filling in forms automatically / suggesting input values
Automatic Choice of Identity	Rule handling and context detection
Pseudonym Management	Support of different pseudonyms
Reachability Management	Managing addressing / allowing of direct connection to communication partner

### 3.1.3 Miscellaneous

*Available:* Statement if the IMA is an available product or service on the market (A), still a prototype (P), a suspended prototype (SP) or just a concept or vision (C).

*Closed/Open System:* "Closed system" means that the IMA/IMS is working only in a completed system environment: The main data flow is carried out only within this system and the IMA has only effects within this system. This is, e.g., the case if an Internet site like ebay.com manages both the member administration and the communication between the members. "Open system" means that the IMA works with several independent systems or applications (cf. Chapter 1.3.4).

*Client/Server (Storage of Identity Data):* Statement whether identity data are stored on a system under main control of the user (client), or whether the storage is on foreign IT systems (e.g., from the provider), so that the user can access it only by interfaces established by the provider (server).

*Specific Functionality (Component):* Specifications about special functionalities or features of the IMA.

**Table 22: Miscellaneous Criteria**

<b>Criteria</b>	<b>Description</b>
Available	A: Available P: Prototype SP: Suspended Prototype C: Concept/Vision
Closed/Open System	<b>Closed:</b> Completed system environment <b>Open:</b> works with different systems / applications
Client/Server	<b>Client:</b> Identity data stored on foreign IT systems <b>Server:</b> identity data stored on user system

Specific Functionality	Special functionalities or features and other remarks
------------------------	---

## 3.2 List of IMA Ordered by Availability and Nations

Table 23: List of Identity Management Applications Ordered by Availability and Nations

Name	Manufacturer	Nation	Available
DASIT	Fraunhofer Gesellschaft	Germany	C
DRIM	TU Dresden	Germany	C
idemix	IBM	Switzerland	C
Kerberos tickets	Div.	Div.	C
KeyNote Trust management	KeyNote	Div.	C
MiCircles	Midentity.com	UK	C
Midentity	Midentity.com	UK	C
OpenPrivacy	OpenPrivacy Initiative	USA	C
OTPW	University of Cambridge	UK	C
P3P	W3C	Div.	C
PRIMA DataManager / IJournal	TU Darmstadt	Germany	C
Privacy Network	ID-Vault	USA	C
Private Credentials	Zero Knowledge / Stefan Brands	Canada	C
Trusted Transaction Roaming Project	The Open Group	Div.	C
WS-Security	IBM	USA	C
ATUS	Uni Freiburg	Germany	P
IDMAN	TU Dresden	Germany	P
LibertyAlliance	Div.	Div.	P
Parkinsonpas	City of Alphen a/d Rijn	Netherlands	P
SAML	Div.	Div.	P
TrustBridge	Microsoft	USA	P
XNS	OneName Corporation / Public Trust Organisation	USA	P
Erreichbarkeitsmanager	Uni Freiburg / Gottlieb Daimler- und Karl Benz-Stiftung	Germany	SP
It's My Profile	Prosumer Corp.	USA	SP
Orby Privacy Plus	YouPowered	?	SP
Playboy Privacy Pass	Playboy	USA	SP
SafeZone	Incognito	USA	SP
TrueSign	Privador	Estonia	SP
AccountCourier	Courion	USA	A
Anonymizer Privacy Manager	Anonymizer	USA	A

AssureAccess	Entegrity	USA	A
Certification Authorities	Div.	Div.	A
ClearTrust	RSA Security	Ireland	A
Cookie Pal	Kookaburra Software	USA	A
CookieCooker	TU Dresden	Germany	A
Digital Handshake	iLumin	USA	A
Digital Identity	Ascio Technologies	Denmark	A
Digital Signature Certification	Verisign	USA	A
DigitalMe	Novell	USA	A
Dotomi	Dotomi	Israel	A
eBay	eBay.com	USA	A
eTrust	Computer Associates	USA	A
Every.one.name	Global Name Registry	UK	A
eWallet	Gator	USA	A
FINEID	Population Register Centre	Finland	A
Flirtmaschine.de	Matchnet	Germany	A
Freedom	Zero Knowledge Systems	Canada	A
Freever	Freever	France	A
GetAccess	Entrust	USA	A
Hushmail	Hushmail.com	Canada	A
ID2	Nexus AB	Sweden	A
iPrivacy	iPrivacy	USA	A
Keon	RSA Security	USA	A
Lotus Notes	Lotus	USA	A
ManageID Suit	Blockade	USA	A
Match	Match.com	USA	A
Meetup	Meetup	USA	A
Mozilla 1.4	Mozilla / Open Source	Div.	A
Netidentity	Netidentity	USA	A
NetKey	Kobil	Germany	A
NetPoint	Oblix	USA / UK	A
Outlook Express 6 (Internet Explorer 6)	Microsoft	USA	A
Passport	Microsoft	USA	A
Persona	Persona	USA	A
PGP / GnuPG	Div.	Div.	A
PingID	PingID	USA	A
Policy Manager	Omniva / Disappearing	USA	A
Privacy Companion	IDcide	USA / Israel	A
Privacy Manager	Tivoli Systems / IBM	USA	A
Private Payments	American Express	USA	A
Roboform	Siber Systems	USA	A
Secretmaker	Secretmaker.com	USA	A

---

SelectAccess	Baltimore Technologie	Ireland	A
SiteMinder	Netegrity	USA	A
Shibboleth	Open Source	USA	A
Spamex	SaferSurf.com	Germany	A
Speednames	Ascio Technologies / Speednames	Denmark	A
Sun One / Network Identity	Sun	USA	A
The Sims Online	Electronic Arts	USA	A
There	There.com	USA	A
Upoc	Upoc	USA	A
Vanquish	Vanquish	USA	A
v-Go Single Sign-On	PassLogix	USA	A
VigilEnt	netiQ	USA	A
Viral	Another.com	UK	A
Virtual ID Card	University of Texas	USA	A
X/MCARE	ICL/Simac/McKesson HBOC	Netherlands	A
Yodlee	Yodlee	USA	A

### 3.3 Alphabetic List of IMA

**Table 24: List of Existing Identity Management Applications**

Name	Closed / Open System	Client / Server (Storage of Identity Data)	Access Management	Form Filling	Automatic Choice of Identity	Pseudonym Management	Reachability Management	Specific Functionality / Component
AccountCourier	Open	C/S	Y	N	N	(Y)	(Y)	Automated account provisioning and user ID management (mainly for organisations)
Anonymizer Privacy Manager	Open	Client	N	N	N	(Y)	(Y)	Allows user to customise an individual privacy and security level for each site
AssureAccess	Open	C/S	Y	N	N	(Y)	(Y)	Access management software for Java/J2EE-based web, portals, and web services (for application developers)
ATUS	Open	Client	N	N	Y	Y	N	Choice between different partial identities
Certification Authorities / PKI	Open	C/S	N	N	N	Y	(Y)	E.g., Telesec.de, Verisign.com etc.
ClearTrust	Open	C/S	Y	N	N	N	N	Web access management
Cookie Pal	Open	Client	N	N	(Y)	N	N	Cookie manager
CookieCooker	Open	Client	(Y)	Y	(Y)	Y	N	Exchange of cookies, management of different identities, and form filling
DASIT	Open	C/S	N	N	N	Y	(Y)	Privacy control functionality for e-Commerce
Digital Handshake	Open	Client	(Y)	(Y)	N	(Y)	N	US standards-based electronic signature solution
Digital Identity	Open	Server	Y	N	N	(Y)	Y	Implements SOAP and supports relevant standards such as SAML
Digital Signature Certification	Open	C/S	(Y)	N	N	(Y)	N	Various PKI providers
DigitalMe	Open	Server	Y	Y	N	Y	N	Control of personal information presented to the public or single persons (meCard)
Dotomi	Closed	C/S	(Y)	N	N	(Y)	(Y)	Users can specify the vendors from whom they wish to receive communication in advertising space on the web
DRIM	Open	Client	(Y)	N	(Y)	Y	(Y)	Comprehensive concept based on IDMAN, SSONET etc.
eBay	Closed	Server	N	N	N	(Y)	(Y)	Auction community in the web with own reputation system
Erreichbarkeitsmanager	Closed	Client	N	N	(Y)	Y	Y	Implementation of reachability management on Newton MessagePads
eTrust	Closed	C/S	Y	N	N	(Y)	N	Modular suit for user provisioning, single sign-on and authentication for business
Every.one.name	Open	Server	N	N	N	(Y)	(Y)	Provides e-mail addresses to customers for use by themselves from a pool of second level domains
eWallet	Open	Client	Y	Y	N	N	N	Form filling and password management
FINEID	Open	C/S	(Y)	N	N	N	N	Identification card with digital signature
Flirtmaschine.de	Closed	Server	N	N	N	(Y)	(Y)	Dating agency working with pseudonyms
Freedom	Open	Client	N	N	N	N	(Y)	Services include spam blocking, cookie management, anonymous surfing, and Internet content filtering service
Freever	Closed	Server	N	N	N	(Y)	(Y)	Mobile community management (chat) over SMS, MMS, WAP, and voice
GetAccess	Open	Server	Y	N	N	(Y)	(Y)	Provides organisations with single sign-on to web portal applications
Hushmail	Open	C/S	N	N	N	(Y)	(Y)	Web-based e-mail and document storage system with block lists, auto-responders, different e-mail domains, and digital signature verification
ID2	Open	C/S	(Y)	N	N	N	N	Digital identification solutions on the Internet based on PKI and smart card technology
idemix	Open	Client	(Y)	N	(Y)	Y	N	Anonymous credential system
IDMAN	Open	Client	N	N	(Y)	Y	(Y)	Component of DRIM for management of identities resp. pseudonyms
iPrivacy	Open	C/S	N	N	N	(Y)	Y	Enables consumers to surf and purchase online anonymously, use different unique e-mail addresses and receive products without revealing names, addresses, or credit card information to the merchant
It's My Profile	Open	Server	N	N	N	(Y)	(Y)	Site allows the user to control information about own activities and preferences, e.g., to authorise e-mail contacts from advertisers in relation to these activities
Keon	Open	C/S	(Y)	N	N	(Y)	N	Enterprises can issue and manage their own web server SSL certificates, relying on a third party
Kerberos tickets	Open	C/S	Y	N	N	N	N	A unique key (a so-called ticket) is assigned to each person that authenticates to the network
KeyNote Trust management	Open	C/S	Y	N	N	(Y)	N	Provides a single, unified language for both local policies and credentials
LibertyAlliance	Open	C/S	Y	N	N	-	-	Developing open standards for network identity
Lotus Notes	Open	C/S	Y	N	N	N	(Y)	Management of communication and administration of information flow
ManageID Suit	Open	Server	Y	N	N	(Y)	N	User life cycle management and automation solution for organisations

Match	Closed	Server	N	N	N	(Y)	(Y)	Dating agency working with pseudonyms
Meetup	Open	Server	(Y)	N	N	(Y)	(Y)	Organises local interest groups
Micircles	Closed	Server	(Y)	N	N	N	Y	Phone / SMS equivalent of using mailing lists
Midentity	Open	Server	(Y)	N	?	?	?	Manage how to share digital information & content with other people
Mozilla 1.4	Open	Client	Y	Y	(Y)	(Y)	(Y)	Browser with e-mail client
NetIdentity	Open	C/S	N	N	N	(Y)	(Y)	Providing different e-mail addresses with different domain names to users
NetKey	Open	Client	(Y)	N	N	Y	N	Possibility to manage different digital signatures
NetPoint	Open	C/S	Y	N	N	N	N	Unites enterprise identity management and web access control
OpenPrivacy	Open	C/S	Y	N	N	Y	N	Collection of software frameworks, protocols, and services providing a cryptographically secure and distributed platform for creating, maintaining, and selectively sharing user profile information
Orby Privacy Plus	Open	Client	N	Y	(Y)	N	N	P3P features
OTPW	Open	Client	(Y)	N	N	N	N	A one-time password login capability
Outlook Express 6 (Internet Explorer 6)	(Closed)	Client	Y	Y	N	(Y)	(Y)	Browser with e-mail client
P3P + APPEL	Open	C/S	N	N	(Y)	(Y)	N	Platform for Privacy Preferences (P3P) - standard for matching privacy policies / A P3P Preference Exchange Language (APPEL)
Parkinsonpas	Open	C/S	(Y)	N	N	N	N	Care and security card for Parkinson and chronic disease patients
Passport	Open	Server	Y	N	N	N	N	Single sign-on service
Persona	Open	C/S	(Y)	N	N	N	(Y)	Acts as a user-driven information broker between the consumer and a website; supports P3P and cookie management
PGP / GnuPG	Open	Client	N	N	N	Y	N	Cryptographic software for encryption, decryption, and managing different key pairs for different e-mail addresses
PingID	Open	C/S	Y	N	N	N	N	Independent and open system that interoperates with .Net Passport and Liberty Alliance
Playboy Privacy Pass	Closed	Server	Y	N	N	N	N	Single sign-on solution for websites with erotic content
Policy Manager	Open	Client	N	N	N	N	Y	Allows organisations to automatically control the distribution, confidentiality, and retention of e-mail and attachments
PRIMA DataManager / IJournal	Open	Client	N	N	(Y)	Y	N	Manages history of personal data that a user has transmitted to service providers
Privacy Companion	Open	Client	N	N	(Y)	N	N	Allows automated cookie decisions based on the site's P3P policy
Privacy Manager	Open	Server	N	N	(Y)	N	N	Helps organisations to build privacy policies and practices into their e-business applications and infrastructure (supports P3P)
Privacy Network	Open	?	N	N	(Y)	(Y)	N	Privacy tools for B2B with support of P3P and APPEL
Private Credentials	Open	C/S	(Y)	N	N	Y	N	Pseudonyms that contain no information that can be linked to the identity of their holder
Private Payments	Open	Server	Y	N	N	N	N	Using a random, unique number for each online payment
Roboform	Open	Client	Y	Y	N	(Y)	N	Password manager, form filler, password generator
SafeZone	Open	Server	N	N	N	(Y)	Y	Customers buy and receive products without revealing their names, addresses, or credit card information to the merchant
SAML	Open	C/S	(Y)	N	N	(Y)	N	Standard which defines user authentication, entitlements and attribute information in XML documents
Secretmaker	Open	Client	N	N	N	(Y)	N	Anonymiser that exchanges specific information of the computer with "phantoms" before it is released to the Internet
SelectAccess	Open	C/S	Y	N	N	N	(Y)	Web access control and authorisation management product for organisations
SiteMinder	Open	Server	Y	N	N	(Y)	(Y)	Authentication and authorization management and providing single sign-on for organisations
Shibboleth	Open	Client	Y	(Y)	(Y)	Y	N	Supports inter-institutional sharing and controlled access to web available services with privacy info monitor for the user
Spamex	Open	Client	N	N	N	Y	(Y)	Hides the user's e-mail address and uses disposable e-mail addresses
Speednames	Open	Server	N	N	N	Y	(Y)	Represents providers for domain name registration for building an Internet identity (cf. [Dyson 2002a])
Sun One / Network Identity	Open	Server	Y	N	N	(Y)	N	Account management and organisation identity management
The Sims Online	Closed	Server	N	N	N	Y	Y	Game / Virtual Residence simulation with chat function
There	Closed	Server	N	N	N	Y	Y	Game / Virtual Residence simulation with chat function
TrueSign	Open	C/S	(Y)	N	N	N	N	Secure verification of digitally signed electronic documents
TrustBridge	Open	C/S	Y	N	N	(Y)	N	Enable organisations to share user identities across business boundaries
Trusted Transaction Roaming Project	Open	C/S	(Y)	N	N	N	N	Aims to leverage the existing mobile telephony infrastructure to provide evidence of identity and payment capabilities

<b>Upoc</b>	Closed	Server	(Y)	N	N	(Y)	(Y)	Mobile (chat) service with group function for SMS or WAP
<b>Vanquish</b>	Open	Client	N	N	N	N	Y	Control of e-mail against spamming; definition of authorised senders
<b>v-Go Single Sign-On</b>	Open	Client	Y	N	N	N	N	Single sign-on by taking any form of authentication, including passwords
<b>VigilEnt</b>	Open	Server	Y	N	N	N	N	Automates active directory administration in organisations
<b>Viral</b>	Open	C/S	N	N	N	(Y)	(Y)	Provides e-mail addresses to customers for use by themselves from a pool of characterising second level domains
<b>Virtual ID Card</b>	Closed	Server	(Y)	N	N	(Y)	N	Enables a member of a university community to display own identification credentials to chosen university entities
<b>WS-Security</b>	Open	C/S	N	N	N	N	(Y)	Enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication
<b>XI(M)CARE</b>	Closed	Server	N	N	N	(Y)	(Y)	Privacy-enhanced database system for patient records; three main domains of patient data could only be linked by leading doctor or in case of emergency
<b>XNS</b>	Open	C/S	-	-	-	-	(Y)	Open XML-based protocol for identifying and linking any resource participating in any kind of digital transaction
<b>Yodlee</b>	Open	Server	Y	N	N	Y	(Y)	Different accounts managed by a single user interface

### 3.4 Summary

In this paragraph, the existing IMA were listed in alphabetic order and sorted by availability and country. The function scope of the applications was determined by use of *operational areas* (access management, form filling, automatic choice of identity, pseudonym management, reachability management) as well as *miscellaneous* (available, closed / open system, client / server regarding storage of identity data, anonymity and specific functionality).

The compilation shows that most of the available applications supporting identity management (39 units) derive from the USA; 15 applications come from Europe. With respect to concepts and prototypes, the picture is different: 5 come from the USA, 10 from Europe.

Considering the operational areas access management and form filling are very popular. The manufacturers attend less to automatic choice of identity, pseudonym management and reachability management and fulfil mostly only parts of that functionality.

The most important systems from this list will be compared in the next Chapter.



## 4 [CHAPTER D: FULL SCALE COMPARISON OF THE MAIN SYSTEMS]

To compare IMA, the following grid of attributes has been developed and amended. Related work for specific IMA has been taken into account [Köhntopp 2001; Zehentner 2002; Art. 29 DPWP 2003]. During the test which last several months, the developed grid has been applied.

### 4.1 Grid of Attributes

#### 4.1.1 Overview

The following grid of attributes is the result of the basic requirements and mechanisms discovered before. Every functionality will be analysed under the main categories of usability, security, privacy, law enforcement and trustworthiness. The grid is completed by details and descriptions of the platform and environment with respect to the effort for the user and operator.

**Table 25: Description of Functionality**

Functionality	Description
IMS Category	Operational areas, purposes, main function / interfaces
Representation of Identities	Personal data, pseudonyms, credentials and their data
Handling of Identities	Definition, verification, implicit & explicit choice and (re-) use of identities
History Management	Logging of transactions of the IMA
Context Detection	Detection of context / suggestions for further activities
Rule Handling	Automatic decisions of the IMA
Privacy Control Functionality	Technological support for giving information about stored personal data, allowing access to these data, giving the means to correct these data, to remove them, or to grant or revoke consent
Identity Recovery	Possibility of recovery an identity, e.g., after a system crash
Digital Evidence Functionality	Preserve evidence for legal proceedings

**Table 26: Description of Categories**

Categories	Sub-Categories	Description
Available and Extent		Function available / extent of realisation
Usability	Perceived Usefulness	System benefits user in an organisational context
	Perceived Ease of Use	How using a system would be free of effort
	Malfunction Understanding	Ability to present a risk of faulty operation / warn him / help him to avoid it
Security	Confidentiality	How and how far confidentiality is ensured
	Integrity	How integrity and authentication are ensured
	Availability	Availability in case of unexpected incidents
Privacy	User Empowerment	IMA supports the user to discover his privacy rights
	Transparency	Transparency of functions referring to privacy rights
	Data Minimisation	Reduction of processed personal data; use of pseudonyms / anonymity; unlinkability
Law Enforcement		Possibility of digital evidence

and Liability		
Trustworthiness	Multilateral Security	Segregation of power, self-protection, open source etc.
	Seals	Privacy and other seals that certify that IMA apply to law

**Table 27: Description of Platform and Environment**

Platform and Environment	Description
Hardware, Software Services	Description of needed hardware, software, OS and services including the costs
Installation	Installation process, Maintenance, Training and costs
Technical Resource Requirements	E.g., number of people needed for operation and costs
Scalability	E.g., user base – estimated scale factor
Availability	Distributed, available, prototype, concept, idea or vision
Installation base IMS	Number of users
Interoperability	Standards etc.
Guarantee for Trustworthiness	For the entire IMA and the manufacturer
Legal and Contractual Framework	Of IMA/IMS and manufacturer and considered legal system
Nature of Provider	Like public, private, regional, national, international

## 4.1.2 Functionality

### 4.1.2.1 IMS Category: Operational Area, Purposes and Functions/Interfaces

Describes the purposes the IMA/IMS could be used for, and the operational areas such as access management, form filling, reachability management, automatic choice of identity and pseudonym management<sup>155</sup>. Additionally interfaces to other systems or applications, protocols, plug-ins and gateways are listed.

### 4.1.2.2 Representation of Identities: Personal Data, Pseudonyms, Credentials and their Attributes

Describes which mechanisms the IMA/IMS uses for showing the user his/her different kinds of identities, especially the one he/she is acting in or the most probable identities to choose from. This includes all possible forms of identities, e.g., plain personal data, pseudonyms, credentials and their attributes.

### 4.1.2.3 Handling of Identities: Definition, Verification, Implicit & Explicit Choice and (Re-)Use of Identities

Describes the functionality of identity handling, meaning identity administration and choice. Identity administration comprises the definition of own identities and the verification of own or foreign identities. Identity choice consists of all possibilities for the user to choose explicitly his/her identities and decide on the re-use of identities and of everything where the IMA/IMS supports the user by seamless use of identities (implicit use) or giving information to help him/her.

### 4.1.2.4 History Management

The history management applies to the logging of all transactions of the IMA. This includes details about what the IMA is logging and how this log file is represented to the user. In connection with the usability-category it is analysed how comprehensible this representation is and if it is useful.

<sup>155</sup> Cf. 3.1.2 Operational Area.

#### 4.1.2.5 Context Detection

This functionality describes possibilities to detect the context of the user's environment and makes suggestions for further activities or executes them autonomously. It has to be described further which contexts the IMA can detect and how the user can affect them.

#### 4.1.2.6 Rule Handling

The rule handling affects the automatic decisions of the IMA. Analysed is which parts of the IMA uses rules, which are default ones, how the user can influence them and if they can dynamically react in case of changing contexts.

#### 4.1.2.7 Privacy Control Functionality

The user could be supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent. This includes mechanisms like P3P or even more direct possibilities to assert one's privacy rights. The extent of privacy control functionality is described in Chapter 2.3.7.

#### 4.1.2.8 Identity Recovery

This functionality helps to recover an identity after a system crash or a malfunction. This could be useful both for the user in case of using a deleted or destroyed identity again and for the law enforcement in case of prosecution. Identity brokers may play a crucial role for identity recovery.

#### 4.1.2.9 Digital Evidence Functionality

Describes if the IMA helps to preserve evidence for legal proceedings. This could be important for users in case of prosecution or claim as well as for law enforcement and criminal prosecution. Analysed is how powerful the evidence would be in a legal proceeding that comes along with the difficulty of manipulate the evidence. E.g., digital signatures and digital time stamps could help to increase the value of the evidence. Another relevant issue is whether the user is aware of the digital evidence functionality and may even influence the kind of digital evidence or whether this is a hidden functionality with no possibility to affect it.

### 4.1.3 Categories

The different mentioned functions are analysed according to the following different categories. The rating system belongs to different essential requirements for this category. For each category five points are allocated at maximum. For reasons of clearness the top categories of security and privacy (with each three sub-categories) in each case are integrated into one rating category with fifteen points at maximum.

#### 4.1.3.1 Available and Extent

Describes if the function is actually available. If so, the extent of its realisation is analysed.

#### 4.1.3.2 Usability

The usability aspect describes both the usability of the product and the documentation and external support.

---

### **Perceived Usefulness**

The construct of perceived usefulness means a person's perception of using an information system that benefits him or her in an organisational context. It is the degree to which a person believes that using a particular system would benefit his or her tasks.

### **Perceived Ease of Use**

The degree to which a person believes that using a particular system would be free of effort. Perceived usefulness and perceived ease of use have influence on the actual use of the IMA.

### **Malfunction Understanding**

Describes the ability to present the risk of faulty operation to the user to warn him and help him to avoid it. This could be an additional warning request that the user has to reply or the ability to undo a malfunction after the user understood that he did something wrong.

### **Rating**

Usefulness (max. possible: 5 points):

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- Time for first time adjustment is less than time for action without IMA: (+1)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

Ease of Use (max. possible: 5 points):

- The help function is not needed for standard activities: (+0.5)
- The manual is not needed for standard activities: (+0.5)
- Help function, manual and support are not needed at all: (+1)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (+0.5)
- A complete and understandable manual is provided: (+0.5)

Malfunction Understanding (max. possible: 5 points):

- The user can recognise that an error occurred: (+1)
- In case of a malfunction the function presents a complete and understandable description of the error: (+2)
- There are suggestions for what to do next: (+1)
- The function makes a sensible suggestion about what to do next: (+1)

### **4.1.3.3        Security**

To analyse security it is necessary to distinguish between different kinds of data. This could be personal data entered by the user stored in a database, personal data transferred to a third person, data for configuration of the IMA which includes the rules for administration of the identities, log data of previous activities or data that is no personal data but can be used for building profiles.

### **Confidentiality**

Describes how and how far confidentiality is ensured, e.g., the level of protection against hacking and data theft from outside of the IMA/IMS.

**Integrity**

Describes how and how far integrity and authenticity are ensured, e.g., the protection of data against illegal destroying and manipulation. Manipulation could be prevented or identifiable, e.g., with use of digital signatures. Also non-repudiability is analysed.

**Availability**

Analysis of the availability of functions in case of unexpected incidents. The availability can be assured, e.g., with backup-solutions, redundancy, third persons etc.

**Rating**

- The stored data is encrypted: (by default: +2 / optional: +1)
- Transmitted data is encrypted: (by default: +2 / optional: +1)
- Data access and manipulation is only possible after authentication: (by default: +2 / optional: +1)
- There are known bugs which could be security-relevant: (-2)
- There are patches / revisions (+1)
- There are immediately effective patches / revisions without side effects (+1)
- Stored data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (by default: +2 / optional: +1)
- Transmitted data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (by default: +2 / optional: +1)
- The availability is supported by redundancy and / or fault-tolerant mechanisms: (+1)
- Backup & restore of data is supported: (+1)
- Backup & restore of data is (manually) possible with adequate effort: (+1)
- Fall-back solutions and / or external services for security are provided: (+1)
- IMA informs completely about all processed and transmitted personal data: (+1)

**4.1.3.4 Privacy****User Empowerment**

Analysis if and how the IMA supports the user to discover his/her privacy rights for using them. The presentation of privacy could be with additional text messages, documentation or even external education. The user should be able to perform self-protection.

**Transparency**

Describes the transparency of the function referring to the kind of user and his/her privacy rights. This means if and how the user can understand and reconstruct the activity of the investigated function.

**Data Minimisation**

Means the reduction of processed personal data by anonymity and pseudonymity procedures, minimising the linkability between a person and the personal data. Describes if more personal data is processed than necessary for the system / application.

**Rating**

- There is a privacy policy: (+1)
- Privacy issues (law etc.) are documented: (+1)
- Privacy issues are well documented inside the IMA (e.g., help function): (+1)
- There are warnings on the occasion of privacy-relevant behaviour: (+1)
- The user has freedom of choices concerning the identity management: (+1)

- 
- The user is supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent: (+1)
  - The IMA informs user about purpose of data processing or does not process personal data: (+1)
  - The IMA informs completely about all used and transmitted personal data: (+2)
  - The IMA adheres to EU privacy standard / privacy statements exist as postulated by the "Safe Harbor Principles" by the US Department of Commerce: (+1)
  - Usage of pseudonyms / anonymity is possible: (+1)
  - Usage of different pseudonyms is supported (+1)
  - User is only asked for needed data overall: (+1)
  - Only necessary data is processed (data minimisation): (+1)
  - Unlinkability / anonymity of data is supported: (+1)

#### **4.1.3.5 Law Enforcement and Liability**

##### **Description**

Describes if the functionality allows law enforcement agencies or other third persons to access the processed data. This could be, e.g., a backdoor or data retention. Analysed is further the utilisation of the collected data.

In case of civil proceedings the value of digital evidences is analysed. This could depend, e.g., on the use of different kinds of digital signatures like qualified or advanced signatures.

##### **Rating**

- There is a history / log function: (+1)
- There are mechanisms for liability and non repudiation in transactions: (+1)
- Time stamping is supported: (+1)
- History / log data accepted by court as evidence: (+1)
- IMA supports the including of a trusted third party as a witness (+1)

#### **4.1.3.6 Trustworthiness**

##### **Multilateral Security**

The trustworthiness of functions can be achieved by multilateral security. Mechanisms for this can be segregation of power, self-protection, separation of the security into different hands and open source, so that only minimal trust in other parties is required [cf. Rannenberg/Pfitzmann/Müller 1996; 1999].

##### **Seals**

Privacy Seals, being a mechanism for trustworthiness, should certify that IT products or services at least apply to privacy protection law (being privacy-compliant) or are even privacy-enhancing. These days a variety of such privacy seals, mostly for specific application contexts like web sites, are available. Some seals have a more general approach, and they try to translate existing privacy regulation into evaluation criteria for IT systems. Some exist purely for marketing purposes.

##### **Rating**

- The IMA provider is an established company being well observed or a federation of independent companies: (+1)
- The IMA is open source (+1)
- The IMA has been evaluated by a formal procedure and issued a seal: (+1)
- The IMA is at least partly under control of the user: (+1)

- 
- The IMA is fully under control of the user: (+1)

#### **4.1.4 Platform and Environment**

##### **4.1.4.1 Hardware, Software, Services**

Description of the hardware, software, operating system and services the IMA/IMS needs including the costs being used as a benchmark criterion.

##### **4.1.4.2 Installation, Maintenance, Use (Training)**

Description of the installation process and use of the IMA including an analysis of the costs from acquirement until complete usage of maintenance and training.

##### **4.1.4.3 Technical Resource Requirements**

Describes the technical resources that are necessary, pointing out the number of people needed for operation and the costs.

##### **4.1.4.4 Scalability**

The scalability of the system when, e.g., the user base grows is described by an estimated scale factor.

##### **4.1.4.5 Availability**

Statement about the availability of the IMA/IMS. It could be distributed, available, prototype, concept, idea or vision. If it is a system in operation, the up-time and the guaranteed availability will be described.

##### **4.1.4.6 Installation Base IMS**

Number of users of the IMA/IMS.

##### **4.1.4.7 Interoperability / Standards**

Description if the IMA can be used with other applications and systems. This could be achieved by using standards like protocols for communication.

##### **4.1.4.8 Guarantee for Trustworthiness**

Description of the guarantees for the trustworthiness of the IMA/IMS. This is not obtained to the single functionality, but to the entire IMA and mainly to the trustworthiness of the manufacturer. Seals of third parties may be described here.

##### **4.1.4.9 Legal and Contractual Framework**

Description of the legal and contractual framework of the IMA/IMS and the manufacturers. Analysis of the considered legal systems and their legal specifics.

##### **4.1.4.10 Nature of Provider**

Description of the nature of the provider of the IMS/IMA like public, private, regional, national, international.

## 4.2 Evaluation of Identity Management Applications

The most popular and trend-setting approaches of Identity Management Applications have been analysed and evaluated. These cover the detected operational areas and have been mentioned by the experts of the survey: Outlook Express of the Microsoft Internet Explorer, Mozilla Navigator and Microsoft Passport are the most popular applications with identity management functionality<sup>156</sup>. Liberty Alliance is the biggest competitor to Microsoft Passport with more partners and a focal point on trustworthiness and privacy. Yodlee has a different approach to Passport and Liberty Alliance as it merges different accounts under one user interface. CookieCooker is more than only a form manager but can administrate random identities also. For presentation of identities in relation to choosing of different roles Novell Digitalme is a precursor.

Table 28 shows which Identity Management Applications are being compared and what their main functionalities / operational areas are.

**Table 28: Compared Identity Management Applications and General Functionalities**

Identity Management Application	Operational Area	Mainly analysed Functionalities
Mozilla Navigator	Access Management Form Filling Reachability Management (Automatic Choice of Identity) (Pseudonym Management)	Form Manager Password Manager
Microsoft Passport	Access Management	Single Sign-In
Liberty Alliance	Access Management Reachability Management	Single Sign-In
Novell Digitalme	Access Management Form Filling Pseudonym Management	MeCard Access Manager Form Manager
Yodlee	Access Management Pseudonym Management (Reachability Management)	e-Personalisation
Microsoft Outlook Express	Access Management Form Filling Reachability Management (Pseudonym Management)	Password Manager Form Manager
CookieCooker	Form Filling Pseudonym Management (Access Management) (Automatic Choice of Identity)	Form Manager / Password Manager

In addition some more interesting approaches of Identity Management Application (e.g., projects, concepts and identity management in organisations with reference to the user) have been shortly analysed and are characterised. A compilation is found in Table 29.

**Table 29: Further interesting Approaches of Identity Management Applications**

Identity Management Application	Characteristic
Freiburg iManager / ATUS	Supports partial identities and their choice
DRIM (TU Dresden)	Comprehensive concept based on IDMAN, SSONET etc.
Sun One	Identity management based on different services
Digital Identity	Implements SOAP / supports relevant standards such as

<sup>156</sup> Google Hits 09/03: "Internet Explorer": 8,840,000; "Outlook Express": 2,580,000; ".Net Passport": 2,390,000; "Mozilla": 9,450,000; "Liberty Alliance": 83,800; "Yodlee": 8,180; "CookieCooker": 10,800.

	SAML
Open Privacy	Collection of software frameworks, protocols and services providing a cryptographically secure and distributed platform for creating, maintaining, and selectively sharing user profile information
IBM WS-Security	Enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication
American Express Private Payments	Using a random, unique number for each on-line purchase

## 4.2.1 Mozilla 1.4 Navigator

Mozilla<sup>157</sup> consists of five parts: the Navigator, Mail & Newsgroups, IRC Chat, Composer and Address book. The Navigator is the Browser that is responsible for viewing of web pages and FTP directories. Mail & Newsgroups serve the reception, the forwarding and management of e-mails and messages in newsgroups. IRC Chat is a chat application that can access IRC servers. Composer allows the creation of web pages and the Address book handles address data.

The selection from a variety of different pseudonyms is offered by the Navigator, Mail & Newsgroups (incl. address book) and the IRC Chat. Only these parts meet the requirements of an IMA and will be examined.

The Navigator shows two general functionalities of identity management:

1. A form filling function allows the data entry of particular categories (e.g., name, address, credit card no. etc.). This entry can be made by the user themselves by entering the data in the input mask. It is also possible to take over the data from filled-in web page forms. These data will then be stored together with the address of the page. Both options provide the possibility to collect several alternative entries for each term in the form.

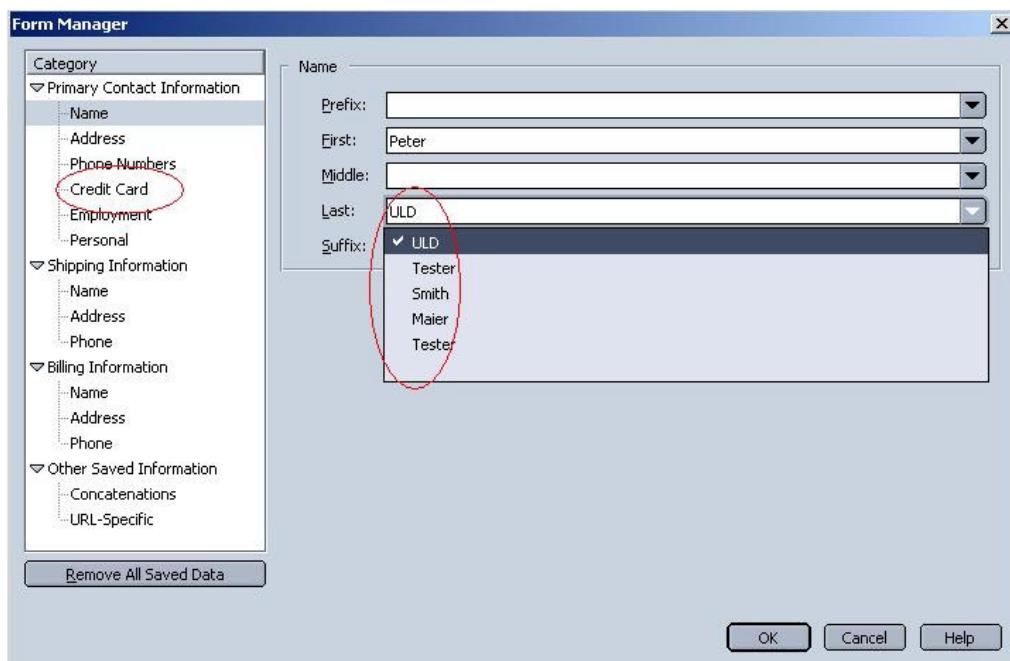


Figure 35: Form Manager with Choice

If a form on a web page requires the entry of data and if its entry lines have the same name as the previously used categories the form manager of Mozilla can be used to enter these terms automatically. This is done by either a double click on the entry line (and Mozilla will then make the entry if there is an entry for this term) or by selecting the "Fill in Form" command from the menu (a window will be opened in which a suggested entry appears for every single line of the form, if applicable). The user can now select alternative entries. Mozilla can also be configured to fill in such forms automatically without asking for verification.

2. The Password Manager serves the management of login data of web pages. As soon as a web page asks for login data (e.g., user name, password) and the user enters these data and confirms, the password manager asks if it is to store these data. Now the user can accept,

<sup>157</sup> <http://www.mozilla.org/releases/>; version tested in this study: <http://ftp.mozilla.org/pub.mozilla/releases/mozilla1.4/mozilla-win32-1.4-installer.exe> (Windows version).

deny or determine that these data are never to be stored. If the user accepts, password manager will store the data (without evaluation of consistency and correctness). When the user visits this site again, the password manager will enter these data automatically in the appropriate fields. If the query process takes place via a special window there will already be the option to select if the data are to be stored for a later use or not.

It is possible to use different profiles for different users of the Navigator. This allows saving of different preferences settings, passwords, form entries etc. under different names. For the communication to the outside this has no added value regarding to identity management.

This profile system in connection with the cookie manager accomplishes identity management functionality. The cookie manager is used to control and manage cookies. Cookies are small bits of information used by the majority of commercial web sites. When a web user visits a site that uses cookies, the site might ask the browser to place one or more cookies on the hard disk. This cookie can contain information like an ID number, visited web pages, form entries etc. Later, when the user returns to the site or web page, the browser sends back the cookies that belong to the site. Cookies are used to transfer information between different web pages (e.g., the cart of a web shop) or for later visits (e.g., recognition of things ordered before). The cookie manager allows watching and deleting cookies stored on the own computer. However its main purpose is to control, which cookies should be allowed and which should be rejected. The user can set different privacy levels for different kinds of cookies. If available, Mozilla uses P3P privacy policies.

#### **4.2.1.1      IMS Category: Operational Area, Purposes and Functions/Interfaces**

Both the Form Manager and the Password Manager can be deployed for several purposes in content, therefore they meet the requirements of a multi-purpose IMA. They are limited to the web services, however, and cannot be deployed cross service. This means that they can be used for all web pages that carry out queries via web forms or extra windows, independent of the pages' purposes.

#### **4.2.1.2      Representation of Identities**

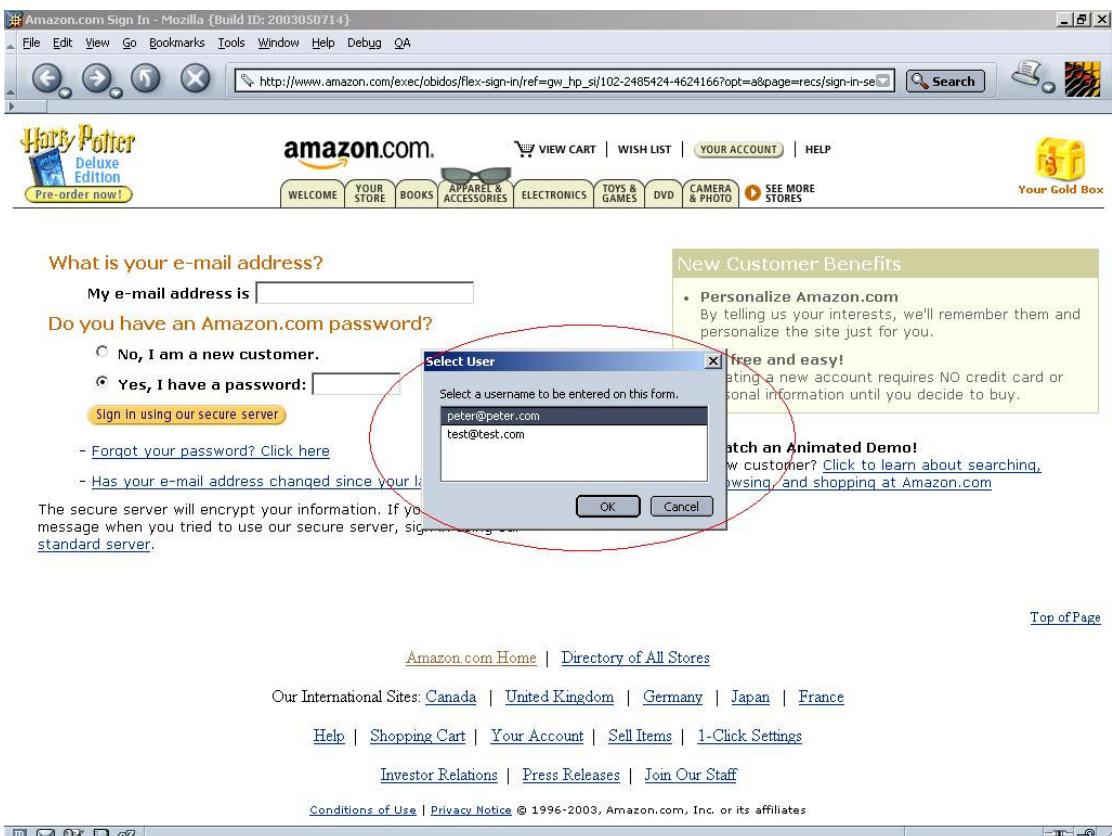
The representation of identities takes place via unchanged data the user has entered once. An application-controlled pseudonym generation does neither exist in the Form Manager nor in the Password Manager. There is also no option to import data records and pseudonyms from outside.

In the Form Manager, multiple alternative entries can be made for every form entry without any possibility to create and manage one's own various pseudonyms and data profiles. In Mozilla, the number is only limited to the technical capacities.

#### **4.2.1.3      Handling of Identities**

In the Form Manager, the partial identities are created and entered by the user. The user is always in control if and which of the partial identities are to be used by making a choice in the appearing window, rejecting it or deleting and overwriting suggested entries. All entries (every single one or as a whole) can be deleted by the user.

In the Password Manager, the entry of the login data takes place by filling in the user name and the password in the appropriate fields of the access query. The Password Manager will store these data if the query has been accepted. When the user visits the web page the next time, the Password Manager will fill in these fields automatically. If the user overwrites these entries and enters other data, which they also store, they will be able to choose between these different access data at their next visit.



**Figure 36: Password Manager and Possibility of Selecting a User**

All entries made by the Password Manager (every single one or as a whole) can be deleted by the user. A manual procedure in the application is not included; it must take place via deletion and new entry

#### 4.2.1.4 History Management

Neither the Form Manager nor the Password Manager include a history function that is adjusted to their functionality, i.e., the use of pseudonyms and data sets will not be stored in a way that the user can view or evaluate later. The Navigator itself as a browser includes a history function. The pages visited by the user will be stored with date and time of the visit and the complete URL of the page. These data can be searched and sorted by day, time and URL. The data entered by the Password Manager or the Form Manager, the management context and the time will not be recorded.

#### 4.2.1.5 Context Detection

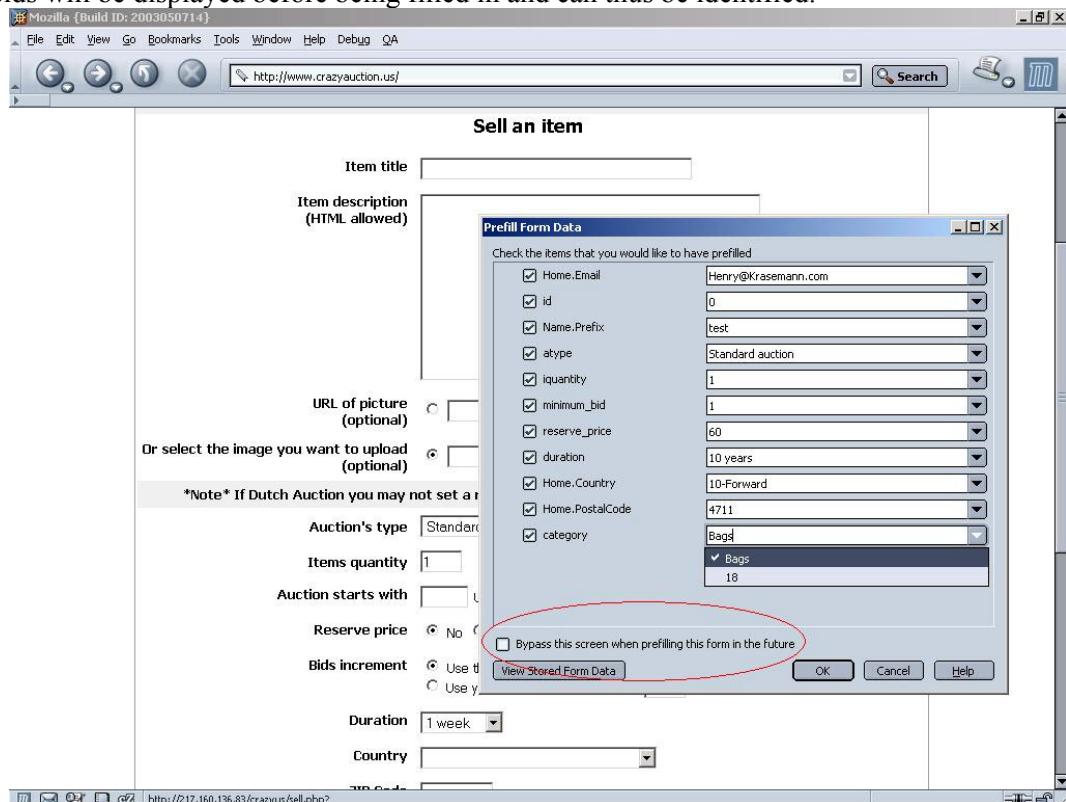
Both the Form Manager and the Password Manager detect form lines by their name within the form definition of the HTML page.

#### 4.2.1.6 Rule Handling

The first definitions for rules, which can be set by the user is the decision if the Form Manager or the Password Manager will be deployed at all. Further on, the user can decide if the Manager is to be deployed for individual web pages. In cases of multiple selection options, the Form Manager allows the user to choose a favourite entry, which will then be entered as the first suggestion. Further on, the user can decide if the Form Manager is to make entries automatically or only on request.

#### 4.2.1.7 Privacy Control Functionality

The users are not specifically supported in asserting their privacy rights such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent. Both the Form Manager and the Password Manager support the users in protecting their data by displaying the data they enter in the forms. The users must activate the sending procedure. This diminishes the risk of sending personal data unintentionally, also in cases in which the Manager is configured to enter the data automatically. There is still the risk, though, that data are entered in hidden fields (credit card no. etc.) without the user's knowledge. If the automatic entry option is deactivated, the hidden fields will be displayed before being filled in and can thus be identified.



**Figure 37: Form Manager – Possibility to Fill in Automatically**

The Navigator supports the W3C standard P3P. P3P is especially deployed for the handling of cookies (see above). Further on, it is possible to view the policy of the visited web page via the command "View – Page Info". This includes also the allocation of the P3P information in a text in the language selected by the user.

The form and password manager will enhance the privacy protection of a user by making it easier to use different passwords and different pseudonyms for different logins. Without such a manager many people use the same password for most of the sites they are registered on. This increases the risk of misuse of data.

#### 4.2.1.8 Identity Recovery

Functions for the recovery of data do not exist within the Form Manager or the Password Manager. If data are being deleted they cannot be restored again. The only possibility would be to backup manually stored data records and call them up again later. However, Mozilla does not support this.

---

#### **4.2.1.9      Digital Evidence Functionality**

A Digital Evidence Functionality concerning the Form Manager or the Password Manager does not exist in Mozilla. The entries can be modified at will; modifications cannot be proved later.

#### **4.2.1.10     Categories**

##### **Usability – Perceived Usefulness**

The Form Manager facilitates the filling-in of forms easier for the user. Entry of default data can be accelerated, and at least a rough overview over the used pseudonyms is provided. Even complex data such as credit card numbers, social security numbers or various phone numbers can be easily selected without having to look them up first. This simplification only refers to the form queries in which the names correspond to those the Form Manager can recognise. In cases of divergence, the user has to make the entries, which is not unusual due to some web designers' lack of compliance with standards when programming forms. Only after filling in various web pages for several times, the recognition rate can be increased. This problem does not exist if the form entries of a page are stored directly and another visit follows. In this case, the entries will be recognised correctly. However, most forms are filled in only once by the same user.

The Password Manager always refers to actually visited pages of which the access data are being stored. If the entry of a password has been recognised and stored once it will be entered correctly on the following visits. For the user, this means an acceleration of the data entry because the only thing left to do is activating the sending button. In addition, the manual management of passwords can be left out.

Rating:

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

##### **Usability – Perceived Ease of Use**

The function of the Form Manager is generally understandable for the user. According to the default configuration of the Navigator, the user will be asked if the form entries to be sent are to be stored. The filling-in of forms requires some additional knowledge from the user, though, e.g., that the automatic filling-in of the entire form can be activated via a command in the menu bar.

Considering the help file the user can get these instructions easily. Under the topic "Using the form manager" he gets this information fast. All steps for using the form manager are presented and comprehensible. Risks like the automatic filling in are mentioned and solutions suggested.

According to the default configuration, the Password Manager, too, asks the user if the entered login data are to be stored. When the user visits the page again, these data will be entered automatically if they have been stored. Thus, no additional information will be required from the user.

Further information is presented in the help file, too. The topic "Using the Password Manager" tells the user the main topics about using this feature. The presentation is similar to the form manager.

Rating:

- The help function is not needed for standard activities: (+0.5)
- The manual is not needed for standard activities: (+0.5)
- Help function, manual and support are not needed at all: (+1)

- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (+0.5)

### **Usability – Malfunction Understanding**

The form manager fills in the form even in automatic mode without sending it to the provider of the web site. For the user it is possible to control all entries before pressing the send-button. Only if there are hidden fields it is thinkable that the user can not see in automatic mode what the form manager enters in a field (see above).

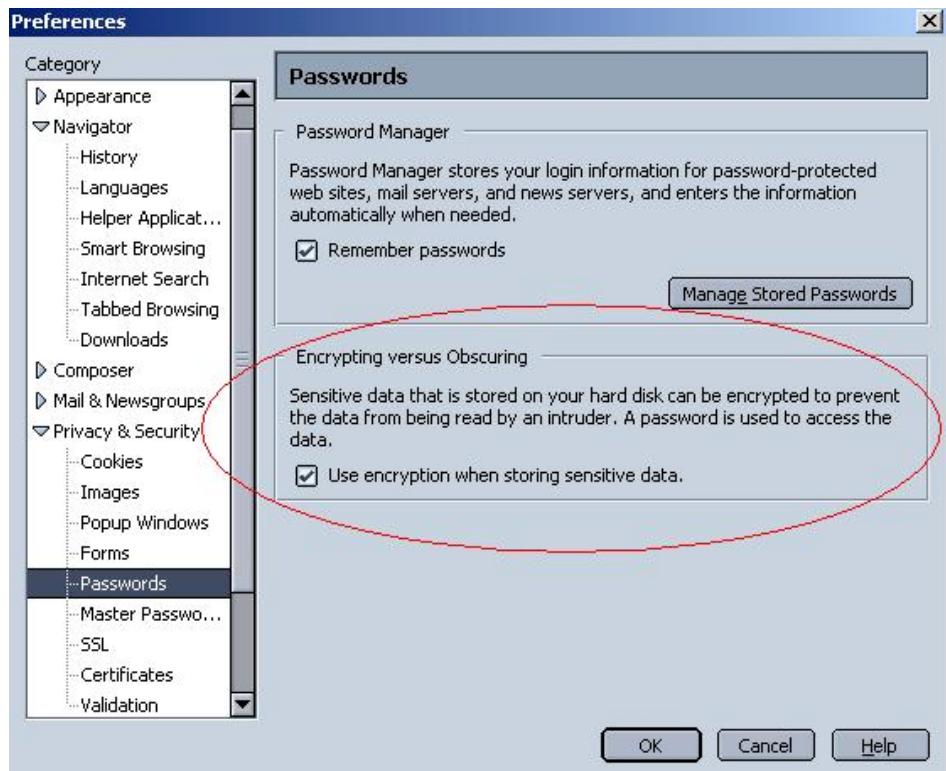
Rating:

- The user can recognise that an error occurred: (+1)
- In case of a malfunction the function presents a complete and understandable description of the error: (+2)
- There are suggestions for what to do next: (+1)

### **Security – Confidentiality**

By default, the form manager and the password manager store data unencrypted. As a result parts of the data, like the names of the affected web sites, are stored in plain text, which can be read by everybody with access to the computer. Passwords themselves are obscured, but can be translated into plain text without much effort.

His preference settings allow the user to activate "use encryption when storing sensitive data". The pre-setting is a "Password Based Encryption With SHA-1 and 3-key Triple DES-CBC" which guarantees a higher security level. This means that not even parts of the files are encrypted but also a master password is used. When using the form or password manager after activating the encryption, it is necessary to enter this master password when using one manager. But the names of the web sites are stored as plain text anymore. A hacker wouldn't be able to read the passwords of the user but he would know where he is registered. This is insufficient for a desirable, high level of privacy.



**Figure 38: Encryption When Storing Sensitive Data Activated**

As the data is stored on the PC the user has better control over access to this data. There is no possibility of direct access from the outside to the user files implemented. The risk of intentionally built-in backdoors by the programmers is reduced, because Mozilla is an open source project where the source code is ready to be controlled by everybody. But outside attacks are not impossible. In particular plug-ins such as JavaScript or ActiveX, which can execute foreign programs on the system, can produce security problems. The only device left to the user is then disabling or uninstalling them.

For secure transfer of data the navigator maintains Secure Sockets Layer (SSL) connections. This requires that the connected web site support SSL too. SSL is a protocol that allows mutual authentication between a client and a server for the purpose of establishing an authenticated and encrypted connection. SSL runs above TCP/IP and below HTTP, LDAP, IMAP, NNTP, and other high-level network protocols. Mozilla also supports the new standard of the Internet Engineering Task Force (IETF) called Transport Layer Security (TLS) that is based on SSL.

Some TCP/UDP port numbers like 1080, 2080 and 3080 are closed by default for communication to prevent unauthorised access to the system.

### **Security – Integrity**

The support of SSL / TLS allows not only a secure communication and prevents the decoding of the transferred data. SSL / TLS assures also the integrity and authentication of the data. However as stated before, it is necessary that both communication partners support it.

### **Security – Availability**

The navigator is a single person system under the complete control of the user. The availability depends on his attitude. There is no redundancy and no backup solution implemented. The user only has the possibility to backup the system files by himself/herself.

### **Security – Rating**

- The stored data is encrypted: (optional: +1)
- Transmitted data is encrypted: (optional: +1)
- Data access and manipulation is only possible after authentication: (optional: +1)
- There are known bugs which could be security-relevant: (-2)
- There are patches / revisions (+1)
- There are immediately effective patches / revisions without side effects (+1)
- Transmitted data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (optional: +1)
- Backup & restore of data is (manually) possible with adequate effort: (+1)
- IMA informs completely about all processed and transmitted personal data: (+1)

### **Privacy – User Empowerment**

The form and password manager itself does not support user empowerment with regards to privacy. Only preferences under the topic of "Privacy & Security" expound the problems of privacy. General help buttons refer to more information. These contain information about using the privacy features of the navigator (Cookie Manager, Password Manager, Form Manager, Managing Images). The topic "Privacy on the Internet" introduces some privacy risks like "What Information Does My Browser Give to a Web Site?" "What Are Cookies, and How Do They Work?" "How Can I Control Web Pages in Email Messages?" and "How Can I Make Sure Unauthorised People Don't Use Information About Me?"

### **Privacy – Transparency**

A user of the form or password manager is not able to see easily where his or her data is saved. He/she has to search on his hard disk for the files. These files only contain the data presented by the functions in an obscured or encrypted way (see above). Beside this observation, the functions are comprehensible.

### **Privacy – Data Minimisation**

Data minimisation – reduction of processed personal data, use of pseudonyms / anonymity, unlinkability – is not in the focus of this IMA..

The user is not obliged to enter any personal data. Every time visiting a web site the Navigator transmits "Mozilla" and its version number as well as the user-agent referrer. These data can be saved in a log file of the web site and analysed later by the web site provider. This is a normal function of a browser according to the HTTP standard. Modification of the user-agent information transmitted is not provided, however additional tools to achieve this are available.

A more important problem is the data request of the form manager. If the user edits the "Form Info", the form contains fields for name, address, credit card number, employment etc. This presentation could suggest the user that he has to fill in all these fields for correct functioning of the manager.

### **Privacy – Rating**

- Privacy issues (law etc.) are documented: (+1)
- Privacy issues are well documented inside the IMA (e.g., help function): (+1)
- The user has freedom of choices concerning the identity management: (+1)
- The user is supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent: (+1)
- The IMA informs user about purpose of data processing or does not process personal data: (+1)
- The IMA informs completely about all used and transmitted personal data: (partly +1)

- 
- Usage of pseudonyms / anonymity is possible: (+1)
  - Usage of different pseudonyms is supported (+1)
  - User is only asked for needed data overall: (+1)

### **Law Enforcement and Liability**

Law enforcement agencies have no access to the data of the navigator without access to the computer itself. The user is generally liable for any use of the data filled in by the form manager or the password manager. With the exception of the hidden fields the user can control all form entries and has to send them manually. There are no additional precautions against identity theft.

Rating: 0 Points

### **Trustworthiness – Multilateral Security**

The trustworthiness of Mozilla is based on its build-up development as open source software. Scores of programmers have created the software as a community collaboration, whereby mutual quality assurance is enabled. The source code is available to everybody for free for review. Security holes can be closed after their detection in a short period of time. It should be noted that the ability to review source code would be of little direct benefit to the overwhelming majority of users. They will however derive an indirect benefit from the collaborative quality process present within the open-source developers community.

### **Trustworthiness – Seals**

No official (privacy) seal certifies the trustworthiness of Mozilla. Because of the ongoing development of this software a seal wouldn't help to increase its trustworthiness to an important extent.

### **Rating – Trustworthiness**

- Open source (+1)
- The IMA is fully under control of the user: (+2)

## **4.2.1.11 Platform and Environment**

### **Hardware, Software, Services**

Mozilla is generally available for Windows (95, 98, ME, NT, 2000, XP), Linux, AIX, HPUX, OpenVMS, OS/2, Solaris and Mac OS 9.x and X. The tested version 1.4 was until 2003-05-22 only available for Windows, Mac OS X, Linux, AIX, OpenVMS and Solaris in different localisations.

There are no further special requirements for soft- and hardware. Around 20 MB free hard-disc space is needed for full installation with all components. Mozilla can be downloaded for free from the Internet<sup>158</sup>.

### **Installation, Maintenance, Use**

The installation process depends on the operating system. For Windows self-extracting ZIP files and setup.exe programs exist that help to install Mozilla. The installation process itself is easy and automated. For Linux, the user can download RPM files depending to the used Linux distribution for easy installation.

---

<sup>158</sup> E.g., <http://www.mozilla.org>.

Updates of Mozilla are able to convert the existing preferences settings of older versions. Mozilla can import some profile data of other browsers like Microsoft Internet Explorer to make the transfer easier in connection with low costs. This import has to be done manually and the user is advised to control the import afterwards in order to check for possible malfunction.

The usage of Mozilla is comparable with other browsers like Explorer, Netscape and Opera etc. and requires no special training. For someone who has worked with a browser before, the main functions are self-explanatory. The on-line help-system can assist the user to learn the functionality of the navigator. It is detailed, comprehensible and easy to access. However, there is no central point of contact for support. A number of sites, newsgroups and mailing lists are available where questions about the program can be placed. This could mean certain enquiry for the user but is only necessary in case of special problems. As the main functions are comparable to other browsers, the costs for support are not assessed as high.

### **Technical Resource Requirements**

Mozilla is designed to be used by single users. No additional resources are necessary for operation.

### **Availability**

Mozilla version 1.4 and older versions are distributed on the Internet.

### **Installation Base IMS**

According to various statistics<sup>159</sup> Mozilla and Netscape cover around 10 % of the browser market.

### **Interoperability / Standards**

Mozilla supports the main W3C and other web site standards like HTML 4.01 and XHTML 1.0/1.1, CSS1, CSS2 and parts of CSS3, DOM1, DOM2 and parts of DOM3 (baseURI, load, and some namespace handling methods), MathML, P3P, XML 1.0, XSLT, Namespaces in XML, XML Base, XLink, Associating Style Sheets with XML Documents, XPath 1.0, FIXptr, RDF, and SOAP.

With plug-ins other standards are or can be integrated like JavaScript, ActiveX, Shockwave etc.

### **Guarantee for Trustworthiness**

As stated before the trustworthiness of Mozilla belongs to its concept of open source. A community of developers helps to make it secure and usable.

### **Legal and Contractual Framework**

The user does not have to agree to a special contract in order to use Mozilla. Parts of the source are available under either the Netscape Public License (NPL) or the Mozilla Public License (MPL), often in combination with either the GNU General Public License (GPL) or the GNU Lesser General Public License (LGPL), or both. Mozilla.org is working towards having all the code in the tree licenced under a MPL/LGPL/GPL tri-licence<sup>160</sup>.

---

<sup>159</sup> E.g., <http://www.cen.uiuc.edu/bstats/latest.html>; <http://www.heise.de/newsticker/data/anw-18.12.02-000/>; <http://www.e-media.at/home/meldung.asp?ID=2231>.

<sup>160</sup> <http://www.mozilla.org/MPL/>.

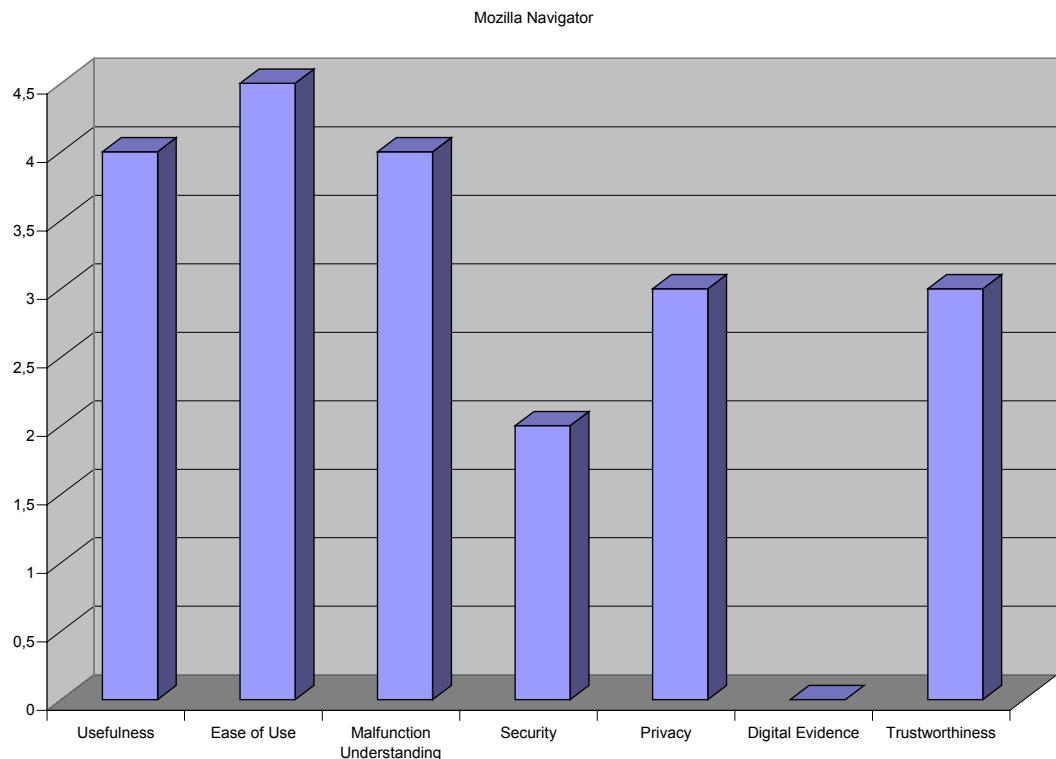
---

### **Nature of Provider**

Mozilla is an open source project with no official distributor or provider. The main contact point is the web site <http://www.mozilla.org/>. There is no additional IMS provider who could manage the user's identities.

#### **4.2.1.12 Conclusion**

The following chart shows the main evaluation results of Mozilla Navigator normalised on 5 points maximum:



**Figure 39: Overview Evaluation Mozilla Navigator**

## 4.2.2 Microsoft .NET Passport

Microsoft .NET Passport<sup>161</sup> is an on-line service via which the user can sign in at any partner site or partner service of NET Passport by use of the e-mail address and a password. This sign-in can take place via the computer at home / at work or appropriately supplied mobile devices. This so-called single sign-in is based on the usage of a pseudonym. Another offspring of this service family (also grouped as .NETmyservices) is .NET Kids Passport, a special single sign-in solution for children with advanced restriction options for parents. The .NET Passport Express Shopping with .NET Passport Wallet has been discontinued as of March 2003<sup>162</sup>.

The user can create a .NET Passport single sign-in account in four ways:

1. By registering at the .NET Passport web site.
2. By registering at a .NET Passport-participating site, which automatically redirects him to a Microsoft-hosted .NET Passport registration page.
3. By registering for an e-mail account through MSN Hotmail or the MSN Internet Access service, which automatically registers him for the .NET Passport single sign-in service.
4. By registering using the Microsoft Windows XP .NET Passport Registration Wizard.

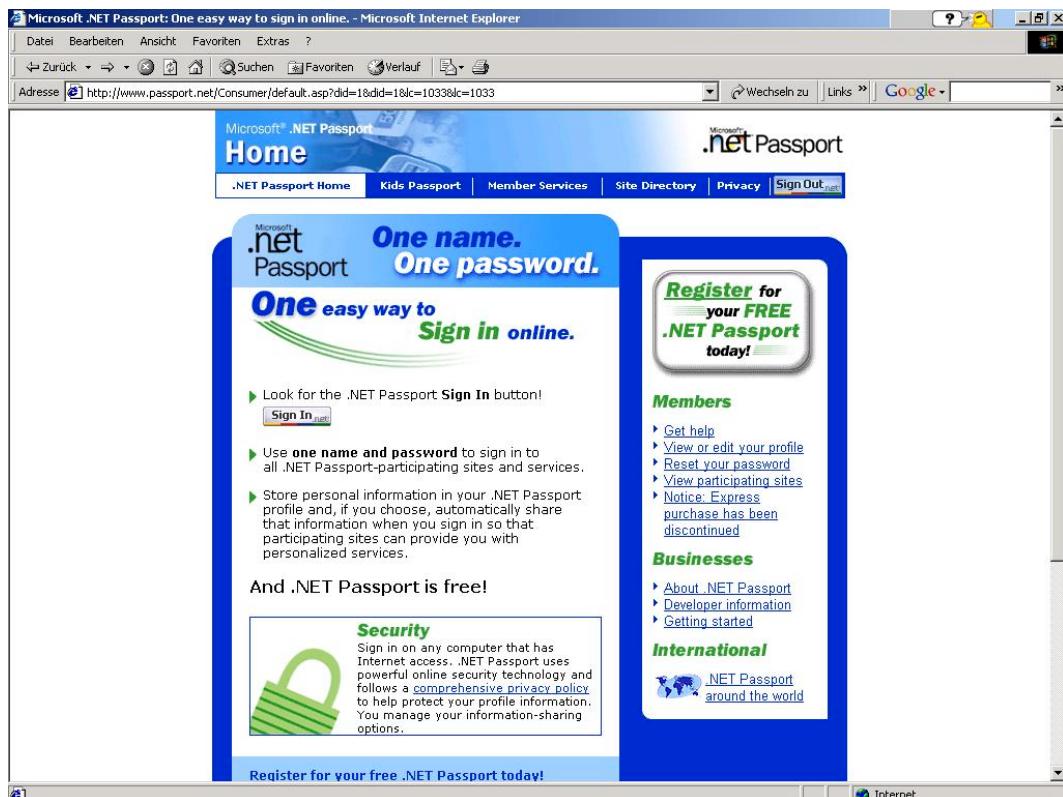


Figure 40: Passport

Kids Passport is a service designed to:

- Provide participating Kids Passport sites with assistance in complying with the parental consent requirements of certain children's privacy laws such as the Children's Online Privacy Protection Act (COPPA).
- Provide parents or guardians a way to manage what .NET Passport profile information their children can share at .NET Passport-participating sites.

<sup>161</sup> This evaluation belongs to the version of Microsoft .NET Passport of September 2003 (i.e. before incorporating changes proposed by [Art. 29 DPWP 2003]).

<sup>162</sup> <http://www.passport.net/Consumer/WalletLetter.asp?lc=1033>.

---

Sites that offer the Kids Passport service may have areas that collect, use, or disclose children's personal information. With Kids Passport, parents can choose – on a site-by-site basis – whether that site can collect their child's personal information, and what the site can do with the information it collects.

Either a parent can register a child for a .NET Passport or a child can create a .NET Passport account on his or her own.

When a parent creates a .NET Passport account for a child, the parent is asked to provide consent to allow .NET Passport to collect and use the child's personal information and to share such information in accordance with the .NET Passport Privacy Statement and the data-sharing preferences contained in the child's profile. That information is then shared with .NET Passport-participating sites where the child signs in.

When a child creates a .NET Passport account, Kids Passport sends the parent an e-mail requesting consent to collect, use, and disclose the child's profile information. Kids Passport does not allow a child to sign in to any .NET Passport-participating site until a parent provides consent.

After a parent provides consent for a child to use Kids Passport, the child will be able to access most .NET Passport-participating sites. However, the child will not be able to access those .NET Passport-participating sites that have implemented the Kids Passport service unless a parent has provided consent for such sites to collect the child's personal information. Parents can provide such consent by reviewing the list of Kids Passport-participating sites, reading each site's privacy policy, selecting which of those sites can receive personal information about their child, and deciding what these sites can do with the personal information they collect. Parents can either grant a specific level of consent or deny consent altogether. In some cases, denying consent for a site to gather personally identifiable information will prevent the child from using a Kids Passport-participating web site.

The European Article 29 Data Protection Working Party made a Working Document on on-line authentication services, adopted on 29 January 2003 [Art. 29 DPWP 2003]. In this document particularly .NET Passport was analysed for conformance to the European data protection law. The result of this document was that .NET Passport agreed in changing some things of their service [PS 2003].

#### **4.2.2.1      IMS Category: Operational Area, Purposes and Functions/Interfaces**

Passport's architecture is a typical client-server system: Microsoft is the IMS provider which centralised server is located outside the (trusted) user area. The Passport server acts as a gateway for all transactions within the system. This means, whenever a user acts within Microsoft Passport, the IMS provider can technically access these data.

MS Passport can be used for multiple purposes. It is not limited to specific applications, but can be used with all web sites, which require an authentication of the user. Additionally the application in mobile services is designated.

#### **4.2.2.2      Representation of Identities**

In the registration process the user is assigned a unique number, the PUID (Passport user ID) which is used later on to identify the user. It is even logged at the Passport server.

For identification and registration the user needs an e-mail address and a password.

According to an announcement by Microsoft, there will be the possibility to create an "anonymous" .NET Passport account some time this year. The user can then choose a user name which does not have to be equivalent to a valid e-mail address [PS 2003, p.6].

#### **4.2.2.3 Handling of Identities**

In the current version of MS Passport, it is only possible to have one identity / PUID per e-mail address. An identity change is only possible after signing in with another e-mail address. The pure authentication requires the e-mail address and password only. However, MS Passport offers the opportunity to enter further data (First Name, Last Name, Country/Region, State, Postal Code, Time Zone, Gender, Date of Birth, Occupation) that will be transferred to a partner site if required. The user can decide to either agree with the transfer or not. Further on, the transfer can be restricted to only a selection of the data by filling in only some of the fields. But, however, the user cannot define different data transfer patterns for the various partner sites.

This, too, is to be changed in the new version of MS Passport, i.e., the user can individually define the data to be transferred to the single partner sites. [PS 2003, p.7].

#### **4.2.2.4 History Management**

MS Passport does not provide any function for the history management. In the members' area, there is still no overview of the partner sites at which the user is or was registered and of the sign-in times.

The only kind of history functions belongs to the MSPVis Domain-Authority Cookie which is written to the passport.com domain. It is used by the Login server to compile the list of sites that must be signed out from when the user clicks any sign-out link. Each new .NET Passport participating site visited has its Site ID written to this cookie which has no encryption.

The user, however, has no direct access to this function nor will the data remain stored beyond the duration of the sign-in. This means that a history management does actually not exist.

#### **4.2.2.5 Context Detection**

If the user has registered with MS Passport and has not activated the option "Do not remember my e-mail address for future sign-in (Select this when using a public computer)", the MSPPre cookie (which contains the user's e-mail address that was used for the sign-in) is created. If the user wants to sign in at a partner site via Passport, this e-mail address will be entered in the corresponding field automatically but can be changed manually. If there was another sign-in within the same session, the e-mail address will be displayed and cannot be changed. Only the password can be entered. The e-mail address can only be changed by activating the link "Not You?".

#### **4.2.2.6 Rule Handling**

A rule handling functionality exists in a way in which the user can choose which of his .NET Passport information can be shared with other companies. He can decide if he wants to share his e-mail address, his first and last names or/and other registration information (Birth Date, Country/Region, State, Postal Code, Gender, Language, Time Zone, Occupation). Up to now, it is not possible to decide individually which data to share with which site. But Microsoft promised to make this possible in a future version (see above).

Another function is the possibility to select "Sign me in automatically" when signing in. If the user selects this check box when he signs in, he remains signed in to his .NET Passport and any participating sites or services until he clicks "Sign Out", even if he closes the browser window or turns off the computer. [.NET Passport recommends in its help file to use this option only if the user is the only person using the computer.]

To sum up, it can be said that there is only a minimum rule handling functionality.

---

#### **4.2.2.7 Privacy Control Functionality**

The users are not specifically supported in asserting their privacy rights such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent.

As mentioned before, the users can choose which of their .NET Passport information can be shared with other companies. They can decide if they want to share their e-mail addresses, their first and last names or / and other registration information (see above). By signing in at [www.passport.net](http://www.passport.net) and choosing the link "View or edit your profile" they are able to see and change their profile at any time.

In a future version of .NET Passport when the users create .NET Passport accounts at a participating site or when they visit participating sites for the first time, they will be asked if they want to share information with the participating site. They will be informed of the country in which the site is located. The site will have space to indicate the purposes for which it wants the information. There ought to be a link to a page that provides more information about how the particular site will use personal information [PS 2003, p. 8].

There is no support of P3P.

#### **4.2.2.8 Identity Recovery**

There is no identity recovery functionality at .NET Passport. After clicking on the link "Close my .NET Passport account" and choosing the button "Close Account" the information stored in the .NET Passport profile will be deleted. If the user decides to reopen his .NET Passport account, he will not be able to recover deleted information.

#### **4.2.2.9 Digital Evidence Functionality**

There is no digital evidence functionality at .NET Passport for the user.

#### **4.2.2.10 Categories**

##### **Usability – Perceived Usefulness**

.NET Passport accelerates the user's workflow, i.e., when signing in at .NET Passport partner sites, the user has to remember only one set of login data (e-mail address and password). If the option "Sign me in automatically" is activated, no additional sign-in at the partner sites is necessary, the user is logged in immediately.

By entering further personal data in the profile and allowing the transfer, the partner sites that need these user data can query them directly. A multiple input by the user, e.g., for the sign-in at different partner sites, is not necessary, which accelerates the workflow again.

Rating:

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

##### **Usability – Perceived Ease of Use**

For using the service of .NET Passport, an initial registration is necessary.

As said before the user can create a .NET Passport single sign-in account in four ways:

1. By registering at the .NET Passport web site.
2. By registering at a .NET Passport-participating site, which automatically redirects him to a Microsoft-hosted .NET Passport registration page.
3. By registering for an e-mail account through MSN Hotmail or the MSN Internet Access service, which automatically registers him for the .NET Passport single sign-in service.
4. By registering using the Microsoft Windows XP .NET Passport Registration Wizard.

The queried data vary, depending on the kind of registration.

**Figure 41: Passport – Profile**

The least data are required for the registration via the .NET Passport website. Only the e-mail address, the password and a registration check have to be entered here. The latter consists of graphically designed letters and numbers that have to be entered manually for the purpose of preventing automated mass sign-ins. Furthermore, the user can decide if the e-mail address may be transferred to the partner sites or not. Finally, the "Microsoft .NET Passport Terms of Use and Notices – AGREEMENT BETWEEN YOU AND MICROSOFT CORPORATION" will be displayed. The user has to choose between "I Agree" or "Cancel". If "I Agree" is selected, the registration is complete.

When registering at a .NET Passport-participating site additional information is requested: Secret Question (like "Favorite pet's name"), Secret Answer, Country/Region, State and ZIP Code. During the registration process for an e-mail account at MSN Hotmail, the first name, last name, language, time zone, gender, date of birth and the profession are asked for, in addition.

**Figure 42: Passport – Registration**

The registration is complete after the data have been entered once. If the user registers, e.g., with ebay.com, the option to connect the .NET Passport account with the eBay account is offered and can be established by a click.

The registration is carried out via a click on the "Sign In" button and the subsequent entry of the e-mail address and the password. The e-mail address will be present in the corresponding field (according to the previous registration).

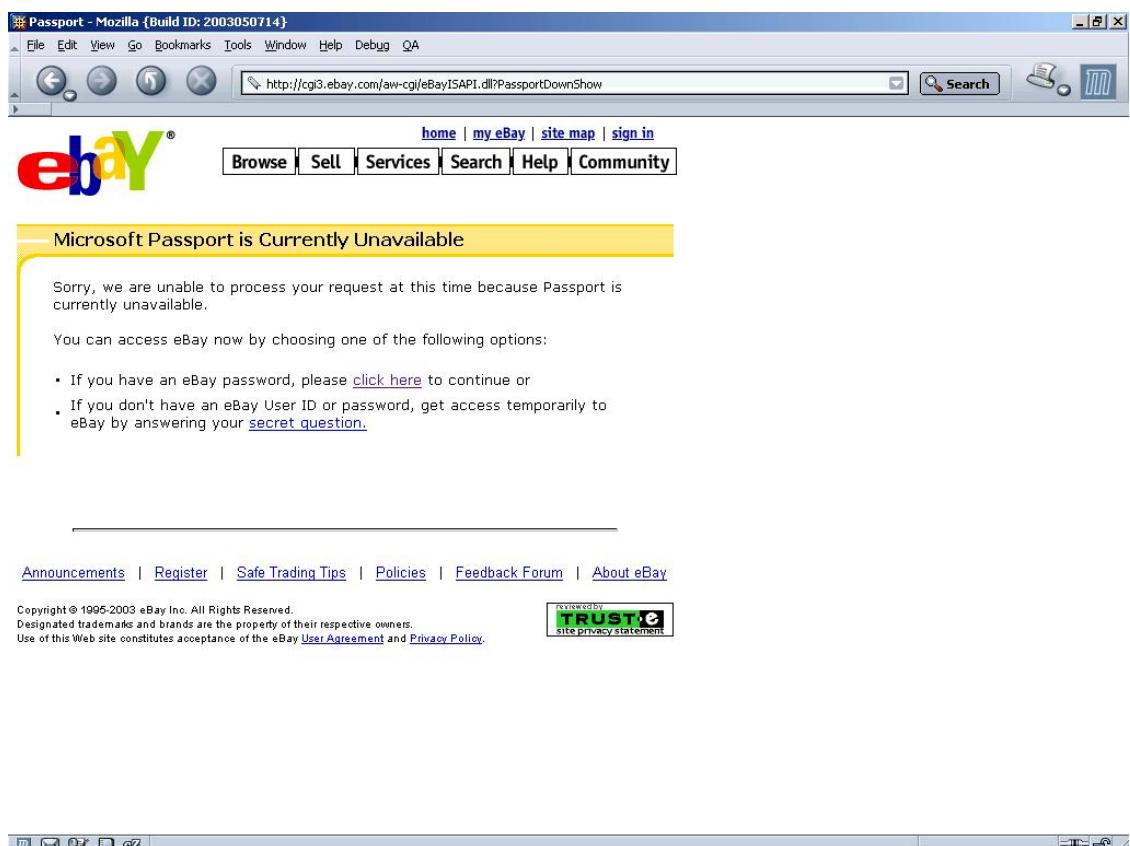
Both the registration with .NET Passport and with the partner sites are therefore simple and easily understandable. The registration needs only a few minutes, the registration with the partner sites is done within seconds.

#### Rating:

- A complete and understandable manual is provided: (+0,5)
- A complete and understandable help function is provided: (+0,5)
- The help function is not needed for standard activities: (+0,5)
- The manual is not needed for standard activities: (+0,5)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0,5)
- No previous knowledge is needed: (+0,5)

#### Usability – Malfunction Understanding

During the test period, problems occurred with the usage of various browsers. While the sign-in always worked with the Microsoft Internet Explorer 5.0, the following message appeared with every sign-in via Mozilla 1.4 at both ebay.com and ebay.de after clicking the "Sign In" button: "Microsoft Passport is Currently Unavailable [...] Sorry, we are unable to process your request at this time because Passport is currently unavailable". Subsequent sign-ins via the Explorer, however, were possible without problems, i.e., this is not a temporary problem as suggested by the error message. The user is lead astray, as far as the malfunction understanding is concerned. The deletion of the cache or the cookies, too, did not help to solve this problem with Mozilla 1.4. The sign-in via www.passport.net, however, was possible with Mozilla 1.4.



**Figure 43: Passport – Malfunction if not using Internet Explorer**

If a mistake is made during the sign-in, .NET Passport points out the error source correctly and offers the user various possible solutions (new attempt, sign-in via the "secret question", new registration etc.).

Rating:

- The user can recognise that an error occurred: (+1)
- There are suggestions for what to do next: (+1)

### **Security – Confidentiality**

.NET Passport includes several different security risks (cf. e.g., [Kormann/Rubin 2000; SLEM 2001]]).

.NET Passport uses 3DES for the data encryption in the cookies that are stored by Passport for further processing. For this, .NET Passport uses a single server key for the encryption off all cookies, which is a security risk [Kormann/Rubin 2000]. The validity period of the server key is limited, though.

3DES is also deployed for the information transfer from .NET Passport to the service providers by use of http redirects. To every partner site, .NET Passport assigns a symmetrical key which has to be transferred to the service provider during the provider registration. According to Microsoft [MS 2000], this key exchange is embedded in an installation program, so that the key is not transferred directly via the internet nor read directly by the system administrators of the partner sites.

.NET Passport requires a definite minimum password length of six characters. Further hints at the selection of a secure password are not given. This can be problematic as the only other access requirement is the user's e-mail address which would be easy to find out for a hacker in most cases.

## Security – Integrity

Early in May 2003, a gap was discovered that has obviously existed since the first version of Passport. This gap enabled third parties to reset passwords of known accounts and define new ones. This requires only a single URL that contained the e-mail address of the account to be changed and the e-mail address of the account to be informed. In the confirmation e-mail from the Passport service, there is a link that allows the definition of a new password. Microsoft disabled the feature while it developed and deployed a fix. As Microsoft says, the vulnerability has since been eliminated and full functionality has been restored to users<sup>163</sup>. In others' opinion, there is still a security problem [Pescarore/Litan 2003].

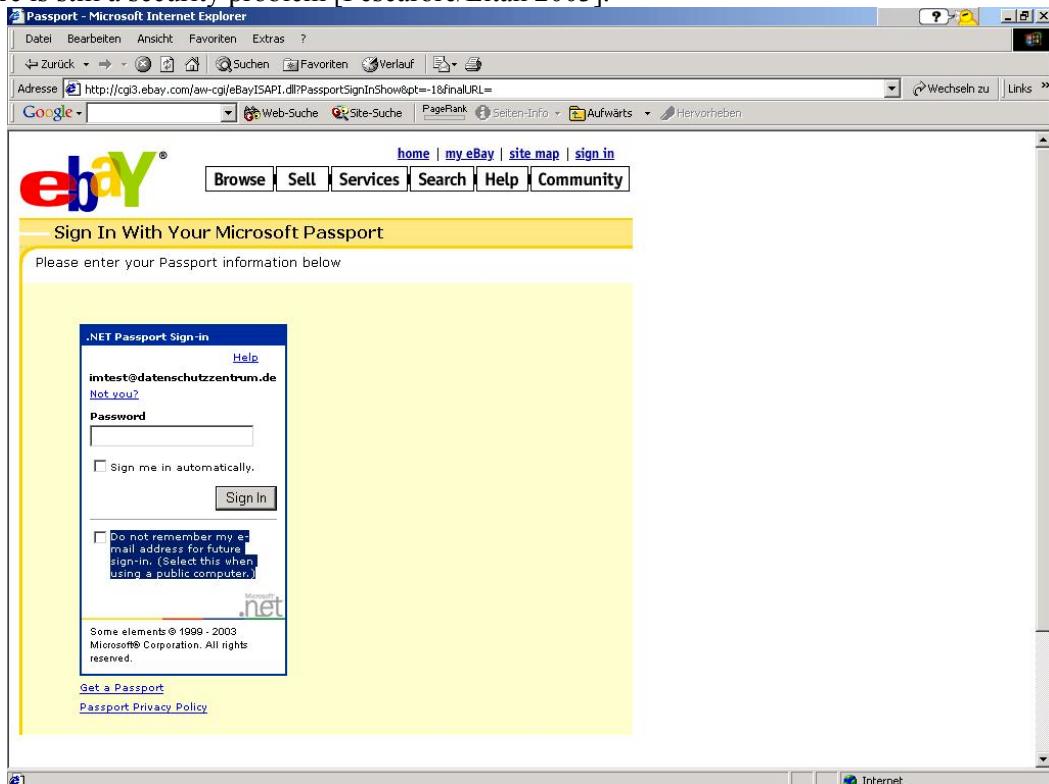


Figure 44: Passport – "Sign me in"

If the user definitely activated the option "Sign me in automatically" during the sign-in process, persistent cookies will be used for the user authentication. The idea is to have a persistent authenticator so that users are not required to retype in their passwords [Kormann/Rubin 2000]. Since with this kind of authentication, an authenticator is missing, owning such a cookie is sufficient for the authentication. Even after the computer would have been switched off and disconnected from the internet, another user could sign in without any further query after establishing a new connection. This causes problems, above all with computers that can be accessed by the public. A solution offered by .NET Passport is the sign-in option "Do not remember my e-mail address for future sign-in (Select this when using a public computer.)". In order to realise the risk of an automated sign-in, the user has to read a second option. There is the risk that the user misses this option when signing in. A definite warning is not displayed after the selection of the automated sign-in. The problem is mentioned in the help text which would have to be called up, though.

## Security – Availability

It remains unknown what internal security measures Microsoft has initiated against Passport server crashes and which back-ups are recorded at which points of time. As long as the original sign-in data at the partner sites (e.g., eBay) are linked to those at Passport, the user can use the specific login data to sign-in at the partner site, even if the .NET Passport server has crashed. If

<sup>163</sup> [http://www.microsoft.com/security/passport\\_issue.asp](http://www.microsoft.com/security/passport_issue.asp).

this is not possible and if there is a long breakdown time, the partner sites can probably give individual access by use of their customer data.

### **Security – Rating**

- Transmitted data is encrypted (by default: +2)
- Data access and manipulation is only possible after authentication: (by default: +2)
- There are known bugs which could be security-relevant: (-2)
- There are revisions (+1)
- Fall-back -solutions and / or external services for security are provided: (partly +1)

### **Privacy – User Empowerment**

If the user indicates in the country field, that he lives in an EU country, a link entitled "Privacy for residents of the European Union" appears below. If the user clicks on the link, a prompt box appears on the side of the page, providing information abutted to the EU data protection law. This box includes a link to the European Commission's data protection page listing countries whose data protection laws have been found by the European Commission to be adequate and comply with EU standards. Included as well is information that .NET Passport keeps the traffic data of the user for no longer than 90 days, unless required to do so by applicable law.

Further notes on the privacy policy of .NET Passport can be found via the link at the bottom of the sign-in page: "TRUSTe Approved Privacy Statement". This leads to the "Microsoft .NET Passport Privacy Statement" hat informs about the following: .NET Passport's Collection of Personal Information, .NET Passport's Use of Personal Information, .NET Passport's General Disclosure of Personal Information, .NET Passport's Disclosure of Personal Information to Participating Sites and Services, Managing Personal Information, Security and Storage of Personal Information, Use of Cookies, .NET Passport and Children, TRUSTe Certification, Enforcement of the Privacy Statement, Changes to the Privacy Statement and Contact Information.

The adherence to the English statement is controlled by TRUSTe, and Microsoft urges the partner sites to allow a control of their privacy protection practices by independent organisations like TRUSTe or BBBOnLine. TRUSTe confirms that Microsoft Corporation is a licensee of the TRUSTe Privacy Program and abides by the EU Safe Harbor Framework as outlined by the US Department of Commerce and the European Union. TRUSTe is an independent, non-profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent. .NET Passport has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe<sup>164</sup>. In privacy information in other languages (e.g., French, German), the note on the control by TRUSTe is missing.

If the privacy statement is changed, this is included in the privacy statement itself. The user has to call up the statement regularly to be informed about possible changes. A notification will not be sent.

As far as the passing-on of profile data that go beyond the actual sign-in data is concerned, the current version of .NET Passport offers only the choice between allowing the transfer or not. The user can still not decide to allow an individual selection of data to be transferred to different partner sites. According to statements by Microsoft, this is to be changed in a future version (see above).

---

<sup>164</sup> Cf. <https://www.truste.org/validate.php?invnum=1135&fromcgi=1>.

---

### **Privacy – Transparency**

The user can select which data are to be transferred to the partner sites. A passing on by default is not permitted, i.e., the user has to be active. Therefore, the user is always informed about which data can be passed on. On the other hand, the user does not know which data are actually passed on to the partner sites.

### **Privacy – Data Minimisation**

Data minimisation – reduction of processed personal data, use of pseudonyms / anonymity, unlinkability – is not in the focus of this IMA..

The registration and usage of .NET Passport currently requires the input of a valid e-mail address. According to Microsoft, the possibility to choose a free user name, which would be data minimisation-friendly, will only be given in a future version (see above). This "Anonymous .NET Passport Account" will include functional limitations, though.

At the sign-in via the .NET Passport page, only the currently required data e-mail address and password are queried. By this, the usage of .NET Passport is possible. With other types of registration (see above), other data will be queried that are not definitely necessary. Particularly the sign-in via Hotmail requires the input of all profile data; the user is not shown immediately what data are necessarily to be entered for the usage of .NET Passport and which ones are voluntary.

After the sign-in at .NET Passport, it is also possible to enter or modify these profile data. The user is notified that these are voluntary statements which are to accelerate the registration with the partner sites.

### **Privacy – Rating**

- There is a privacy policy: (+1)
- Privacy issues (law etc.) are documented: (+1)
- Privacy issues are well documented inside the IMA (e.g., help function): (partly +0.5)
- The user has freedom of choices concerning the identity management : (planned)
- The IMA informs user about purpose of data processing: (+1)
- The IMA informs completely about all used and transmitted personal data: (partly +1)
- The IMA adheres to EU privacy standard / privacy statements exist as postulated by the "Safe Harbor Principles" by the US Department of Commerce: (planned)
- Usage of pseudonyms / anonymity is possible: (planned)

### **Law Enforcement and Liability**

The functions of .NET Passport do not support expressly law enforcement or liability. However, it is at least a technical circumstance that user data and sometimes probably temporary usage data are stored on the servers of .NET Passport. These data could be accessed by law enforcement agencies.

Rating: 0 Points

### **Trustworthiness – Multilateral Security**

Multilateral security is not sufficiently supported. Microsoft .NET Passport manages the user data independently and centrally. The deployed systems and protocols are only partly documented. For example, a cookie called "MSPXPWiz" which is not documented is deployed for the authentication [cf. MS 2002]. Some well-tried security systems such as Kerberos 5 are or will be deployed.

### **Trustworthiness – Seals**

The adherence to the English language privacy statement is monitored by TRUSTe. Further seals for trustworthiness do not exist.

### **Rating – Trustworthiness**

- The IMA provider is an established company being well observed (+1)

#### **4.2.2.11 Platform and Environment**

##### **Hardware, Software, Services**

.NET Passport is an internet service. Its usage requires a computer connected to the internet or an appropriately supplied mobile phone with web access. There are no costs other than those for the internet usage. A usual browser is required which is able to process cookies. During the test period, the .NET Passport registration was possible with Internet Explorer 5, Internet Explorer 6 and Mozilla 1.4. As mentioned above, there were problems with Mozilla 1.4<sup>165</sup>.

##### **Installation, Maintenance, Use**

The installation of special software is not required (see above). The registration with the service is simple and quick (see above), i.e., it will not cause high costs. A training that goes beyond the usual usage of browsers and the internet should hardly be necessary.

##### **Technical Resource Requirements**

The usage of .NET Passport does not require any further technical resources. It is a web service externally operated and maintained by Microsoft.

##### **Availability**

.NET Passport is distributed. During the test period, no downtimes were noticeable; the service was always available. Microsoft does not guarantee availability but claims in its terms of use the right to delete accounts any time without notice ("Microsoft reserves the right, in its sole discretion, to terminate your access to the .NET Passport Services or any portion thereof at any time, without notice").

##### **Installation Base IMS**

The exact number of the real users of .NET Passport is unknown. However, since all Hotmail users are automatically registered with .NET Passport, the number of the (potential) users is to be estimated as high. According to the web page of Microsoft Passport as of November 2003 it has more than 200 million accounts and more than 3.5 billion authentications per month. There are listed 91 web sites using .Net Passport (some by same mother company like ebay.com).

##### **Interoperability / Standards**

For the usage of .NET Passport the usual browsers can be deployed. However, in individual cases, there might be problems (see above). .NET Passport is not compatible with other single sign-on services such as Liberty Alliance or PingID.

---

<sup>165</sup> Cf. [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/passport25/NET\\_Passport\\_VBScript\\_Documentation/Testing\\_And\\_Troubleshooting/Troubleshooting/tshoot8.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/passport25/NET_Passport_VBScript_Documentation/Testing_And_Troubleshooting/Troubleshooting/tshoot8.asp)

---

### **Guarantee for Trustworthiness**

.NET Passport is operated by Microsoft. Thus, Microsoft guarantees the adherence to the privacy directives and the terms of use.

### **Legal and Contractual Framework**

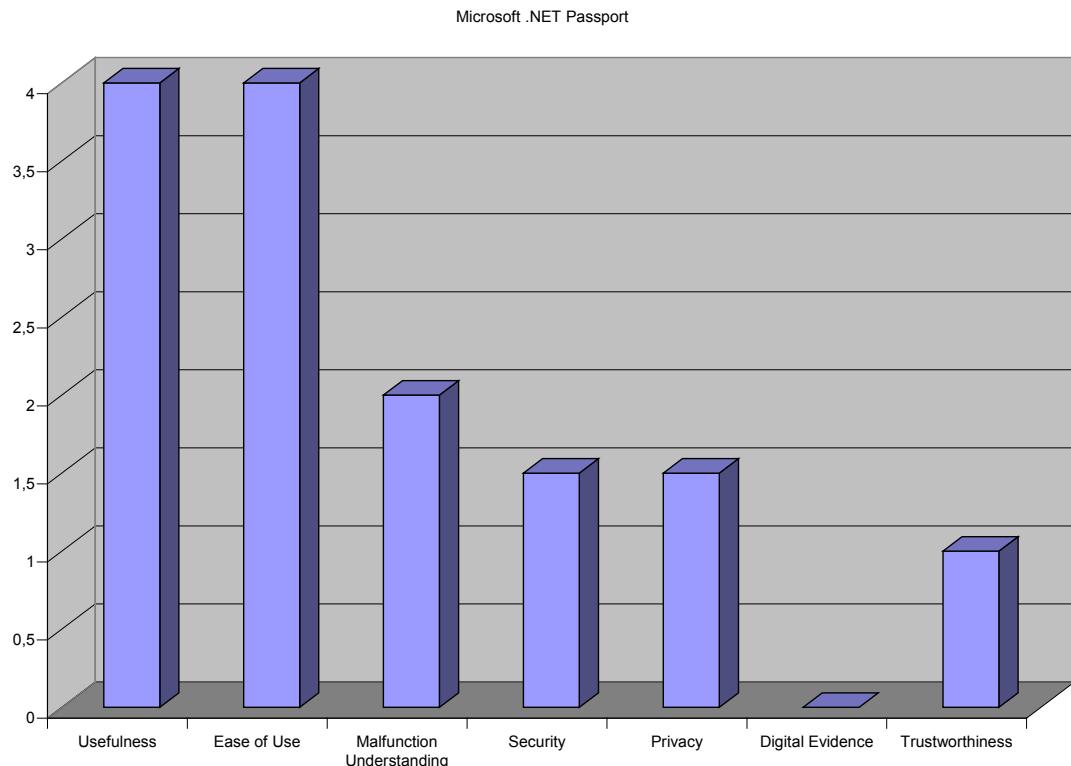
Microsoft, as the operator of .NET Passport, is a world-wide operating group based in the US. There are branches in many countries, e.g., in most of the European countries. In order to be able to cope with the various legal systems the terms of use are partly authored in a very general manner; some parts also consider special national law positions (e.g., the copyright notice in the Terms of Use). If the user gives an EU country when specifying his nationality within the registration with .NET Passport, the registration procedure will be adjusted accordingly, and an additional link with notes for EU citizens will be supplied.

### **Nature of Provider**

Microsoft, as the operator of .NET Passport, is a stock corporation with its central in the US. Microsoft is operating world-wide and has numerous branches and subsidiary companies.

#### **4.2.2.12 Conclusion**

The following chart shows the main evaluation results of .NET Passport normalised on 5 points maximum:



**Figure 45: Overview Evaluation Passport**

### 4.2.3 Liberty Alliance Project

"The Liberty Alliance Project is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way. [...] In a federated view of the world, a person's online identity, their personal profile, personalised online configurations, buying habits and history, and shopping preferences are administered by users, yet securely shared with the organisations of their choosing. A federated network identity model will enable every business or user to manage their own data, and ensure that the use of critical personal information is managed and distributed by the appropriate parties, rather than a central authority. The role of the Liberty Alliance Project in all of this is to support the development, deployment and evolution of an open, interoperable standard for federated network identity. The vision of the Liberty Alliance is to enable a networked world in which individuals and businesses can more easily conduct transactions while protecting the privacy and security of vital identity information."<sup>166</sup>

The idea of a federated network identity results in similar effects as the Microsoft Passport approach, such as convenient single sign-on, but not yet a payment system. Additionally the architecture is designed to support distributed and independent storage units for user data which should be processed according to his decision. Therefore, different circles of trust exist for using such a federated network identity [LA 2003a] (cf. Figure 46), resulting in less vulnerability because of an increased heterogeneity of systems due to independent operators. Circles of trust are a federation of Service Providers and Identity Providers that have business relationships based on the Liberty Alliance architecture and operational agreements and with whom Principals can transact business in a secure and apparently seamless environment.

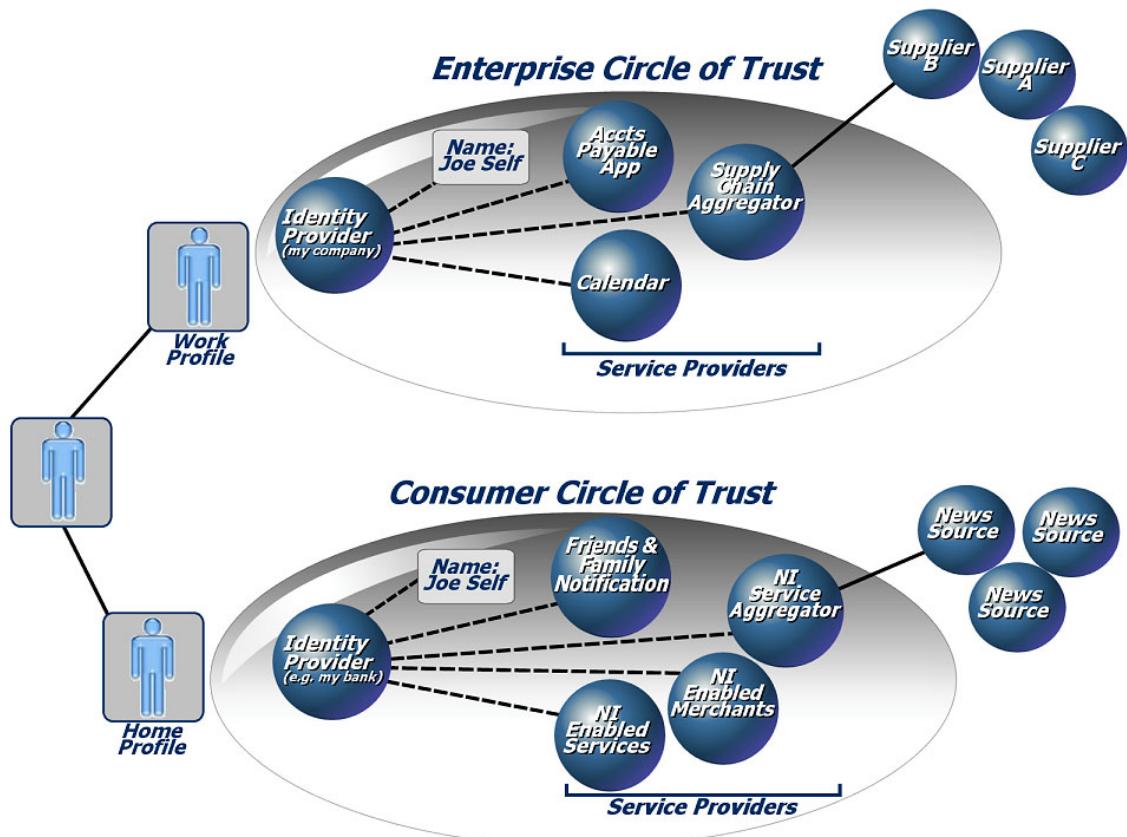


Figure 46: Federated network identity and circles of trust by Liberty Alliance

The Liberty Alliance Project comprises both PC-based and mobile device-based solutions.

<sup>166</sup> <http://www.projectliberty.org/>.

---

Single sign-on is the ability of the consumer to authenticate once in a session with an Identity Provider and later on navigate to various Service Providers within a Trust Domain without having to re-authenticate [Art. 29 DPWP 2003].

#### **4.2.3.1      IMS Category: Operational Area, Purposes and Functions/Interfaces**

The aim of Liberty Alliance is the development of an open, interoperable specification for a network identity within a connection of internet service providers. In this context, Liberty Alliance is to be used by both private and commercial users from different sides with different orientation (multi-purpose), similar to NET Passport.

The users manage their relationships to other instances and their own personal data. In contrast to .NET Passport, the profile information is stored in a distributed way in the form of a non-central user data administration within the company connection.

The user can definitely select which of the accounts at the various service providers are to be connected. A valid user authentication at a service provider will be transferred to those providers at which the user has a connected account. The user is in the position to choose if a sign-off at one provider is to be automatically combined with a general sign-off at all connected providers. In addition, the providers can agree upon the type and the grade of the user authentication to be deployed.

#### **4.2.3.2      Representation of Identities**

The central function of Liberty Alliance is the connection of identities at various service providers. By the connection of the accounts, a group is built (Circle of Trust). A user's sign-in at one provider of the group leads to an authentication at all group members without the user having to enter the required information again. The specification (version 1.2) regulates the management of multiple identities and the passing-on of authentication information.

Liberty-enabled implementations must be able to support the use of pseudonyms that are unique on a per-identity-federation basis across all identity providers and service providers [LA 2003a].

For the designation of identities or for the designation of an identity by use of the transfer within the URL, "nonces" are used. These are random numbers which are believed to practically not being repeated.

#### **4.2.3.3      Handling of Identities**

From the Liberty perspective the actors are the user, service provider and identity provider. Service providers are organisations offering web-based services to users. These could be internet portals, retailers, financial institutions, governmental agencies etc. [LA 2003a, p.7]. Identity providers are service providers offering business incentives so that other service providers affiliate with them. These relationships are the "circles of trust". An identity provider could be a service provider too.

The authentication works like this [LA 2003a, p.33]:

1. The user visits a web site of a service provider
2. He chooses to log in via his preferred identity provider. This login is accomplished by selecting the preferred identity provider from a list presented on the login page of the service provider.
3. The user's browser is redirected to the identity provider with an embedded parameter indicating the originating service provider. The user can then log in to the identity provider as the user normally would.

4. The identity provider then processes the login as normal and, upon successful login, redirects the user's browser back the originating service provider with a transient, encrypted credential ("artifact"), embedded within the URI.
5. The service provider then parses the artefact from the URI and directly uses it to query the identity provider about the user.
6. In its response, the identity provider vouches for the user, and the service provider may then establish a local notion of session state.

As the Liberty Implementation Guidelines recommend identity providers and service providers that support identity federation should also support the Federation Termination Notification Protocol. When supported, both service-provider-initiated and identity-provider-initiated federation termination notification should be supported. Liberty offers two federation termination notification mechanism: front channel (HTTP-redirect-based) and back channel (SOAP-based).

#### **4.2.3.4 History Management**

There is no history function prescribed in the Liberty Architecture. The service provider and identity provider have to decide for themselves to implement this functionality.

#### **4.2.3.5 Context Detection**

Liberty Alliance defines various subclasses of information, named as "Metadata and schemas". The formats and mechanisms for exchanging can vary depending on the subclass. Subclasses of exchanged information are:

1. Account/Identity: Opaque user handle that serves as the name that the service provider and the identity provider use in referring to the user when communicating.
2. Authentication Context: Exchange of information between service provider and identity provider with respect to used technologies, protocols and processes.
3. Provider Metadata: Metadata regarding identity provider and service provider. Includes items like X.509 certificates and service endpoints.

#### **4.2.3.6 Rule Handling**

The implementation and functionality of rule handling belongs to the members of the liberty alliance.

#### **4.2.3.7 Privacy Control Functionality**

The users are not specifically supported in asserting their privacy rights such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent.

Liberty Alliance sees "privacy is security policy applied to a Principal" as a useful model for privacy protection. For them the most relevant security functions needed for privacy are [LA 2003b, p. 13]:

- Authentication of the Principal and/or any other entities that could perform policy management tasks (policy definition, modification, etc)
- Authentication of attribute requesters
- Policy integrity in transit (at the moment of policy definition, modification or any other kind of policy management operation)
- Policy integrity in storage
- Attribute confidentiality in transit (response from the Attribute Provider to the Service Provider)
- Attribute confidentiality in storage

- 
- Attribute integrity in storage and transit
  - Policy management authorisation
  - Audit capability: maintenance of transaction records in secure storage
  - Avoiding collusion between Identity Provider and Service Provider
  - Data aggregation

An integration of P3P has not been planned so far.

#### **4.2.3.8      Identity Recovery**

The identities themselves will still mainly be stored at the service providers. Therefore, the service providers remain responsible for providing a function that allows to restore them after a deletion.

#### **4.2.3.9      Digital Evidence Functionality**

The Liberty Alliance architecture recommends no explicit digital evidence functionality.

#### **4.2.3.10     Categories**

##### **Usability – Perceived Usefulness**

Liberty Alliance allows the simplification of the authentication by the requirement of only one sign –in within the circle of trust to be signed in at other providers, too. There are no other authentication processes with other access data to be carried out. It is also possible to sign off at all connected providers by only one sign-off.

The design of these functions is mainly left up to the members of the Liberty Alliance and belongs to the different realisations.

Rating:

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

##### **Usability – Perceived Ease of Use**

The ease of use belongs to the different realisations of the Liberty Alliance. The given main possibilities to sign-on via Liberty Alliance are the redirect to the web site of the identity provider and embedded forms.

Rating:

- The help function is not needed for standard activities: (unknown)
- The manual is not needed for standard activities: (unknown)
- Help function, manual and support are not needed at all: (unknown)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (unknown)
- A complete and understandable manual is provided: (unknown)

##### **Usability – Malfunction Understanding**

The malfunction understanding belongs to the different realisations of the Liberty Alliance.

Rating:

- The user can recognise that an error occurred: (unknown)
- In case of a malfunction the function presents a complete and understandable description of the error: (unknown)
- There are suggestions for what to do next: (unknown)
- The function makes a sensible suggestion about what to do next: (unknown)

### **Security – Confidentiality**

By use of the technology of the web redirect, there are various possibilities to attack. Web redirection is an action that enables Liberty-enabled entities to provide services via today's user-agent-installed base [LA 2003a, p. 21].

For example, the data can be bugged during the transfer (Interception / Man-In-The-Middle-Attack) [Pfitzmann/Waidner 2002]. The communications go across the wire in clear text unless the data are carried out over an SSL or TLS session or across another secured communication transport (e.g., an IPsec-based VPN). The corresponding infrastructure is provided by Liberty Alliance but, however, there is no obligation to deploy particular security mechanisms. Therefore, the deploying companies are to make sure themselves that the systems they use are secure and show no gaps.

Another security problem could be a user agent leakage [LA 2003a, p. 24]: "Because the channel is redirected through the user agent, many opportunities arise for the information to be cached in the user agent and revealed later. This caching is possible even if a secure transport is used because the conveyed information is kept in the clear in the browser. Thus any sensitive information conveyed in this fashion needs to be encrypted on its own before being sent across the channel."

A service provider can deny the communication with an identity provider if the deployed authentication mechanism or the data transfer protocol fails to meet the security directives. This, however, does not protect from an illegal usage of the service as such.

Within a circle of trust, a common domain is used in which cookies are placed that contains a list of the available identity providers. These cookies can be written by the identity provider and read by the service provider. A security risk comes up when persistent cookies are deployed that remain in existence beyond the communication process. Therefore, Liberty Alliance points out the necessity to give the user the opportunity to select if and which cookies are to be deployed and to warn the user accordingly. The cookies do not contain personal data, though.

### **Security – Integrity**

The meta data and schemes allow the providers to deploy certificates (e.g., X.509) for the authentication to guarantee the user's authenticity. Liberty Alliance does not prescribe a particular certificate / protocol etc. in this context but every circle of trust can choose this according to its own aims and requirements.

Further on, Liberty Alliance points out the possibility of the re-authentication or multi-tiered authentication. This is to be deployed when the user is authenticated in a circle of trust but if a stronger form of authentication is required, e.g., for a financial transaction. In this case the user must present a stronger assertion of identity like public-key certificate. For the adjustment of these differently strong kinds of authentication, the members of a circle of trust are responsible, though.

Further on, the specification requires that the user identity is checked by every service provider. Therefore, the user remains identifiable in an unmistakable way for every provider. The ability to distinguish is guaranteed by the identity provider defining a unique user identity ("Handle")

---

within an identity federation which is stored and exchanged between the identity provider and the service provider.

For the designation of identities or for the designation of an identity by use of the transfer within the URL, "nonces" are deployed. These allow a unique identification without revealing the user's real identity.

Liberty Alliance itself points out that the correct authentication of a fake server is possible via SSL / TLS with the usage of a fake certificate if the user does not recognise the certificate as being a fake. The improvement of the readability of certificates and the simplification of the identification of fakes is left up to the members of Liberty Alliance, though.

### **Security – Availability**

The actual design of the server security and the safe-guarding is left to the members of Liberty Alliance.

### **Security – Rating**

- The stored data is encrypted: (unknown)
- Transmitted data is encrypted: (by default: unknown / optional: +1)
- Data access and manipulation is only possible after authentication: (by default: +2)
- There are known bugs which could be security-relevant: (unknown)
- Stored data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (unknown)
- Transmitted data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (by default: unknown / optional: +1)
- The availability is supported by redundancy and / or fault-tolerant mechanisms: (unknown)
- Fall-back solutions and / or external services for security are provided: (unknown)
- IMA informs completely about all processed and transmitted personal data: (unknown)

### **Privacy – User Empowerment**

The Liberty Alliance protocol is neutral regarding data protection [Art. 29 DPWP 2003].

The presentation of privacy belongs to the service / identity providers. They decide which possibility they give the user to perform do-it-you-self-protection.

### **Privacy – Transparency**

For the Liberty Alliance "simplicity is the main advantage of having only single sign-on, fixed federations, and fixed roles, and this should be reflected by a clear and simple policy" [Pfitzmann 2003]. The specifications define Introduction Data, Authentication Data, Traffic Data, User Attributes.

On the main page of Liberty Alliance ([www.projectliberty.org](http://www.projectliberty.org)), the Privacy Policy of the web site can be viewed. This privacy policy adheres to the international privacy protection standards, i.e., collected data will only be passed on after the user has agreed. Data of minors under 13 years will definitely not be collected. This policy is not fully developed, though. At the place where the user has to click if he does not wish to receive further communications from the Liberty Alliance is only the text-placeholder "add opt-out link".



**Figure 47: Liberty Alliance**

Sun Microsystems, as a decisive company in the Liberty Alliance, and other members are also members of the Online Privacy Alliance<sup>167</sup>. The Online Privacy Alliance is a cross-industry coalition of more than 80 global companies and associations committed to promoting the privacy of individuals on-line. "Its sole purpose is to work over the coming year to define privacy policy for the new electronic medium and to foster an online environment that respects consumer privacy. The group's stated mission is to lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce".<sup>168</sup>

For the Liberty Alliance Project itself, there are the "Liberty Security & Privacy Implementation Guidelines" [LA 2003b] in which the Liberty Alliance points out the importance of a Privacy Policy: "Although it might seem that Principals should define the policies for their personally-identifiable information, in many cases the Identity Provider should also play a central role in this determination. Principals may not be prepared to define policies to control their privacy information in instances where they have not fully understood the privacy implications. [...] The Attribute Provider needs to define some basic/default policies to protect Principal's privacy. These rules should be written in such a way that a Principal has to consciously choose not to use these rules".

### **Privacy – Data Minimisation**

Data minimisation – reduction of processed personal data; use of pseudonyms / anonymity; unlinkability – is not in the focus of this IMA.. By the connection of user accounts within the circle of trust, the single authentication data remain in existence at the individual members.

<sup>167</sup> <http://www.privacyalliance.org>.

<sup>168</sup> <http://www.privacyalliance.org/facts/>.

---

Each of these data can be used for the authentication, which at the same time increases the risk that these data are stolen and provide the opportunity to appear with a wrong identity. Therefore, Liberty Alliance suggests the establishment of a control system for the limitation of these data within the circle of trust. For example, single authentication data could be deleted already with the connection to other accounts or after a certain time period in which the data have not been used.

### **Privacy – Rating**

- There is a privacy policy: (+1)
- Privacy issues (law etc.) are documented: (partly +0.5)
- Privacy issues are well documented inside the IMA (e.g., help function): (unknown)
- There are warnings on the occasion of privacy-relevant behaviour: (unknown)
- The user has freedom of choices concerning the identity management: (+1)
- The user is supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent: (unknown)
- The IMA informs user about purpose of data processing or does not process personal data: (unknown)
- The IMA informs completely about all used and transmitted personal data: (unknown)
- Usage of pseudonyms / anonymity is possible: (+1)
- User is only asked for needed data overall: (unknown)
- Only necessary data is processed (data minimisation): (unknown)

### **Law Enforcement and Liability**

The specification gives no advice for implementation of support for law enforcement or collecting evidences for liability. However, it is at least a technical circumstance that user data and sometimes probably temporary usage data are stored on the servers of service providers and identity providers. These data could be accessed by law enforcement agencies.

Rating: 0 Points

### **Trustworthiness – Multilateral Security**

Liberty Alliance based on Circles of Trust. Requirements of identity provider trust introduction include:

- Identity providers may introduce one another to service providers that they trust, so that new trust relationships may be established in real time.
- Introducing providers may require notification of identity federations that take place as a result of their mediation.
- Notification of service providers when identity providers terminate relationships with one another, allowing the service provider to act according to its own dictates.
- Accommodation of more fluid trust relationships resulting from introductions and terminations [LA 2003a, p. 17].

In contrast to, e.g., Microsoft Passport, there is no central access data management. It is rather the user's responsibility to connect or disconnect accounts between the members of the Liberty Alliance. The specifications of the Liberty Alliance can be viewed in the internet by any user. There are numerous liberties concerning the mechanisms to be deployed, though, i.e., it remains to be seen to which extent the individual members provide information about the realisation of the specifications.

### **Trustworthiness – Seals**

There are no seals for the Liberty Alliance.

**Trustworthiness – Rating**

- No seal and open source etc. unknown / Protocol documented (+1)
- The IMA provider is a federation of independent companies: (+1)

**4.2.3.11 Platform and Environment****Hardware, Software, Services**

Depends on implementation.

**Installation, Maintenance, Use**

Depends on implementation.

**Technical Resource Requirements**

Depends on implementation.

**Availability**

Liberty Alliance is a concept where some prototypes are available (see 4.2.3.12).

**Installation Base IMS**

The Alliance has grown from under 20 companies in 2001 to more than 150 companies in early 2003 (current 09/03: 151).

**Interoperability / Standards**

Liberty Alliance wants to create its own standard. This standard as such is not compatible with other extant standards. However, standardised mechanisms and protocols are deployed (e.g., SOAP, SAML, XML, SSL, TLS etc).

**Guarantee for Trustworthiness**

Liberty Alliance belongs to the circles of trust. This means that members of this circle say that they trust each other. The aim is that when the user trusts one of this group he should trust others too when he logs in there.

**Legal and Contractual Framework**

Many companies within the Liberty Alliance are American-based. The expectation is that the use of the specifications will in practice mean that quite a lot of personal data will be transferred from Europe to the US [Art. 29 DPWP 2003].

**Nature of Provider**

Alliance members represent a world-wide cross-section of organisations, ranging from educational institutions and government organisations, to service providers and financial institutions, to technology firms and wireless providers. In general, all kinds of providers can become members of Liberty Alliance.

---

#### **4.2.3.12      Liberty-Enabled Products<sup>169</sup>**

Cavio Corporation – [www.cavio.com](http://www.cavio.com)

Cavio is transforming its solution to be SAML compliant in order to offer their services as an Identity Provider per the Liberty Alliance specification. Cavio utilises biometrics to secure PKCS11 based soft tokens in a central server architecture to offer a high level of integrity to any Liberty Alliance customer application looking for Authentication Assertions. This solution will give consumers and business users biometric authentication for Internet-based resources, while allowing them to maintain control of their personal information and conduct business with other Liberty-enabled web sites. Cavio's C-Pass product works within the Liberty Alliance framework to provide Authentication Assertions. The C-Sign product allows for the secure non-repudiable digital signing of any web-based transaction. Cavio utilises multiple biometrics and password/PIN combinations in customisable configurations to secure PKCS11-based soft tokens into secure web servers. The combining of these technologies in one solution provides for safe identity management in addition to secure high-integrity identity assertions to Liberty-enabled interested parties. It is expected to ship in August of 2003.

Communicator Inc. – [www.communicatorinc.com](http://www.communicatorinc.com)

Communicator Inc. has implemented the Liberty Alliance version 1.1 specifications into its Hub ID services to create a unified digital identity management service. Communicator Hub ID enables companies to securely extend the digital corporate identities of employees, customers, partners and suppliers beyond the enterprise in a federated manner. This enables identity related services such as single sign-on, self help systems, access to password-protected content and presence management. Communicator Inc is implementing the Liberty Alliance Phase 2 spec in its Hub ID service.

Datakey – [www.datakey.com](http://www.datakey.com)

Datakey CIP is a smart card and interface software package that gives organisations a single device to function as an individual's identity throughout the enterprise – for both data and physical security. With broad support for an enterprise's existing authentication mechanisms, Datakey CIP adds two-factor smart card security for passwords, dynamic passwords, Windows log-on, VPNs, web authorisation, public key encryption, digital certificates and digital signatures. Enterprises benefit from enhanced security for their existing authentication methods while also taking advantage of smart card protection for PKI-enabled applications or simplifying any future migration to PKI. Datakey CIP is currently available.

DigiGAN – [www.digigan.com](http://www.digigan.com)

The DigiGAN Trusted Web Server (TM) (TWS) leverages the multi-level security (MLS) features inherent in a trusted operating system, such as Trusted Solaris, to provide security capabilities not available in any other web server allowing data at different sensitivity levels to be served from the same physical machine, but still maintain security enforced by the kernel-level mandatory access control mechanisms of the trusted operating system. Due to the security features of the underlying operating system, the TWS is not vulnerable to any of the many common attacks against other web servers, such as DoS, brute force, and other defacement attempts by hackers. TWS v2.1 contains support for LDAP, RADIUS, and Kerberos. DigiGAN's Trusted Web Server is expected to support the Liberty Alliance 1.1 specification in the second half of 2003.

Entrust Inc. – [www.entrust.com](http://www.entrust.com)

Entrust plans to integrate the Liberty Alliance version 1.1 specifications into its leading portfolio of security software solutions that provide businesses and governments with the information accountability and privacy they need to transform the way they conduct on-line transactions and manage relationships with customers, partners and employees. Over 1,200 enterprises and government agencies in more than 50 countries use Entrust's solutions that integrate into the broad range of applications organisations use today to leverage the Internet

---

<sup>169</sup> <http://www.projectliberty.org/resources/enabled.html>.

and enterprise networks. Entrust plans to begin integration of the version 1.1 specifications into its enhanced Internet security portfolio in 2004.

Fujitsu Invia – [www.invia.fujitsu.com](http://www.invia.fujitsu.com)

SDA Products – <http://sda.invia.fujitsu.com>

Fujitsu Invia SDA mPollux is designed to secure primarily web and wireless applications. It provides authentication and authorisation services that can be used to control access to a single application, or to implement a Single Sign-On access control system for a variety of applications. Several different user authentication methods are supported, such as PKI, wireless PKI, telephone call or SMS-based authentication. Authorisation functions can be implemented combining the use of mPollux services and the access control features of the web server product in use, or using the optional WebFront Access Control module of mPollux.

Hewlett Packard – [www.jpn.hp.com/hpc/sp/icewall/eng/](http://www.jpn.hp.com/hpc/sp/icewall/eng/)

HP's IceWall SSO is a single sign-on solution that simplifies maintenance tasks for service administrators and allows users to access all the services with a single authentication. It improves existing systems and dramatically decreases the number of processes required in service development and management, while allowing new business models to be developed. It ensures a very high level of security and is flexible enough to permit the development of new business models. HP's ceWall SSO solution is expected to support the Liberty Alliance 1.1 specifications.

July Systems – [www.julysystems.com](http://www.julysystems.com)

July's data services infrastructure software solution – the July Meta-Service System (JMSS) – enables mobile operators to deliver high-value mobile data services to subscribers. JMSS compliance with Liberty Alliance 1.1 specifications allows the operator to take on the value-added role of a federated identity provider, thereby ensuring that subscribers can receive personalised information and transaction capabilities without compromising the privacy of their identity and profile information to application and content partners. JMSS will support features such as authentication context request, name registration request, federation and federation termination request, as well as implement SAML and signature-based message security. July Systems is committed to support all future Liberty Alliance specifications.

NeuStar Inc. – [www.neustar.biz](http://www.neustar.biz)

NeuStar Inc. is built on a foundation of trust and neutrality established over years securely and successfully managing critical registry and infrastructure services for the communications industry. This foundation of trust has set the stage for NeuStar to be a groundbreaking force in offering next-generation infrastructure services including federated digital identity, and the convergence of voice and data networks. As a sponsoring member of Liberty Alliance, [www.projectliberty.org](http://www.projectliberty.org), NeuStar is leading the way with first-of-its-kind, turn-key, Liberty-compliant identity management and federation services. NeuStar's NeuLiberty suite of services offers Trust Circle Administration, Identity & Attribute Discovery Services, and Identity Management Services. NeuStar's NeuLiberty suite of services makes smart business sense in today's competitive market environment. The NeuLiberty services provide a quick, reliable and cost-effective way to support business transactions in a secure network.

Novell Inc. – [www.novell.com](http://www.novell.com)

An early access release of the Liberty identity provider for Novell eDirectory, previously code-named Saturn, is currently available as a free download to customers world-wide. Using the Liberty Alliance version 1.1 specifications, Novell's Liberty identity provider allows businesses to securely establish links among internal, external and partner websites, giving users single sign-on between those websites via open standards. Equally important, the Liberty identity provider allows the users themselves to decide whether their identities will be federated from one web site to another. Offering standards-based single sign-on helps companies drive more value from business relationships, build a more loyal customer base and help employees be more productive.

---

#### Oblix – [www.oblix.com](http://www.oblix.com)

By supporting the Liberty Alliance standards, Oblix NetPoint becomes a single identity management infrastructure that customers can deploy to support multiple, incompatible federated services. Oblix NetPoint has rich capabilities to integrate multiple, external authentication systems and services while providing organisations security and control over authorisation to their valuable applications and content.

#### Phaos Technology Corp. – [www.phaos.com](http://www.phaos.com)

Phaos Technology, the world-wide leader in Java Security, understands the needs of Fortune 500 companies to protect users' privacy and identity. Phaos Technology provides the modular components required by Liberty Identity Providers and Identity Service Providers to build interoperable applications faster, with less complexity. Using Phaos' components, Java developers can create applications that provide important Liberty functionality like: identity/account linkage, simplified sign-on, consolidation of enterprise authentication schemes and integration of legacy systems with XML-based web services.

#### Ping Identity Corporation – [www.pingidentity.com](http://www.pingidentity.com)

Ping Identity Corporation is the sponsor of SourceID ([www.sourceid.org](http://www.sourceid.org)), an open source community that has quickly become the de facto open source implementation for the Liberty Alliance specifications. SourceID SSO is the first component of a larger open source Federated Identity Management System that will be developed and released under the SourceID community. SourceID SSO is designed to make it as easy as possible for companies to participate in Federated Single Sign-On. SourceID SSO focuses on two major capabilities: Liberty Alliance Protocol v1.1 interoperability, and easy deployment for Java web applications. In addition, SourceID intends to integrate all future Liberty Alliance specifications into its open source releases. It is available for free download at <http://www.sourceid.org>. Ping Identity Corporation has also announced the PingID Network, a technology-neutral, member-owned, identity network that helps address the growing inefficiencies and security concerns surrounding the deployment of federated identity services. The PingID Network, which is organisationally modelled after traditional ATM member-owned networks, provides enterprises with the business and legal services they need to enable efficient linking and management of account information between corporations with the end-user's explicit consent. The PingID Network offers enterprises the ability to accelerate their Liberty deployments with its LIVE (Liberty Interoperability Validation Environment) service, and is currently accepting members at [www.pingid.com](http://www.pingid.com).

#### RSA Security Inc. – [www.rsasecurity.com](http://www.rsasecurity.com)

RSA with its Federated Identity tries to bridge the gap between the aforementioned concepts of Microsoft Passport and Liberty Alliance [RSA 2002]. RSA Security plans to support the Liberty Alliance specifications in future versions of its portfolio of identity and access management solutions. RSA Security's Liberty-enabled solutions are designed to allow customers to achieve secure authentication, web access management and single sign-on, both inside and outside of an organisation.

#### Sun Microsystems Inc. – [www.sun.com](http://www.sun.com)

Sun Microsystems offers an end-to-end identity management solution that addresses customers' needs for heightened security, privacy and federated identity management, and is fully compliant with the Liberty Alliance version 1.1 specifications. The Liberty-enabled Sun ONE Identity Server 6.0 provides a complete identity and access management foundation that helps secure the delivery of business information, bridge and consolidate different identity silos, and enables enterprises to manage their users and the user's relationships with the business applications and information. The Sun ONE Identity Server 6.0 is currently shipping.

#### Trustgenix, Inc. – [www.trustgenix.com](http://www.trustgenix.com)

The Trustgenix Federation Server (TFS) enables an enterprise to quickly adopt Liberty 1.1-based identity federation in a minimally disruptive way. The TFS is a J2EE-based server that supports multiple application servers, databases and leading WAP Gateways. It is a scalable and

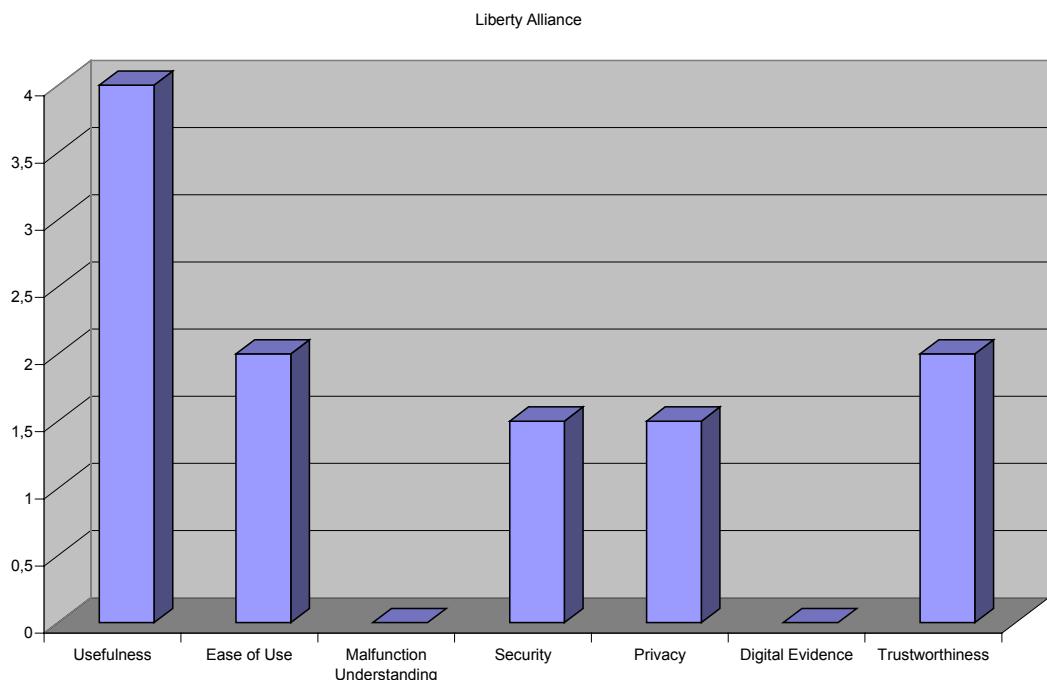
robust platform designed to be rapidly deployed with minimal impact to existing applications. It provides extensive management and workflow capabilities and provides a simple API for integration. Real-world applications have been Liberty-enabled in a matter of less than one week. The server is available for a free evaluation download at [www.trustgenix.com](http://www.trustgenix.com). The Trustgenix Federation Server will soon include features from the Liberty Phase 2 specifications making it even easier for applications to be identity- and data-federation enabled.

WaveSet Technologies – [www.waveset.com](http://www.waveset.com)

Waveset currently supports the Liberty Alliance version 1.1 specifications in its Lighthouse family of identity management solutions. Waveset Lighthouse integrates provisioning management, password management and identity profile management into one solution, leveraging its unique Virtual Identity Manager technology to manage federated identities within and across corporate boundaries. By supporting the Liberty Alliance specification, Waveset extends established security principles like automated provisioning, delegated administration, approval workflow, user self-service and audit and vulnerability detection to the world of federated identity management.

#### 4.2.3.13 Conclusion

The following chart shows the main evaluation results of Liberty Alliance normalised to 5 points maximum (only derived current specifications; concrete implementations of the Liberty Alliance specification could have higher values):



**Figure 48: Overview Evaluation Liberty Alliance**

#### 4.2.4 Novell Digitalme

The free service "Digitalme" by Novell allows the management of digital identities and the related data such as addresses, visited web sites, bookmarks, cookies etc. Digitalme manages relationships with associates, friends, family and e-businesses. As a member, the user has an "always current, accessible-from-anywhere address book, one-click universal information updating, single-click sign-on to password-protected sites and automatic form fill-in"<sup>170</sup>.

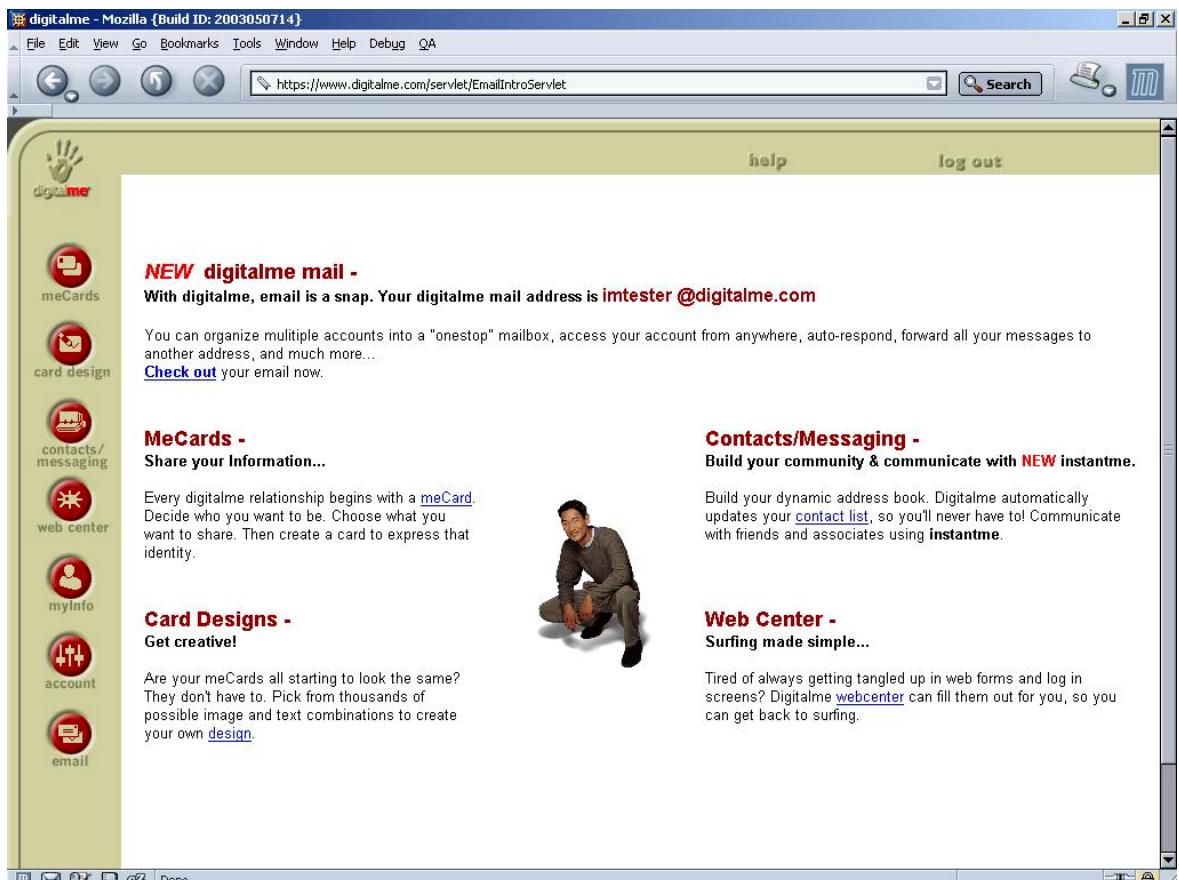


Figure 49: Digitalme

Digitalme is based on Novell Directory Services (NDS) eDirectory 8.5. According to statements by Novell employees, it is some kind of test version to show the opportunities provided by the various identity management and data management systems by Novell. For example, the service was temporarily unavailable in some parts in February 2003, i.e., no new registrations were possible. At the current point of a more specific analysis (June 2003), these disturbances seem to be fixed.

##### 4.2.4.1 IMS Category: Operational Area, Purposes and Functions/Interfaces

The main identity management component of Digitalme is the "meCard". A meCard is a customised personal information profile that the user puts together for a specific on-line purpose. For example, since he'd use them in different situations, his Business meCard would probably have different information – phone, work address, etc. – than his Personal meCard<sup>171</sup>. The user can build as many meCards as he likes, each with personal information and even customised designs, to share with associates, friends and family.

<sup>170</sup> [http://www.digitalme.com/Learn\\_More/](http://www.digitalme.com/Learn_More/).

<sup>171</sup> [http://www.digitalme.com/Learn\\_More/](http://www.digitalme.com/Learn_More/).

Within this context, it is possible to maintain an address book at Digitalme via "contact/messaging". On the one hand, one's own data can be entered, on the other, meCards of other persons can be adopted and managed.

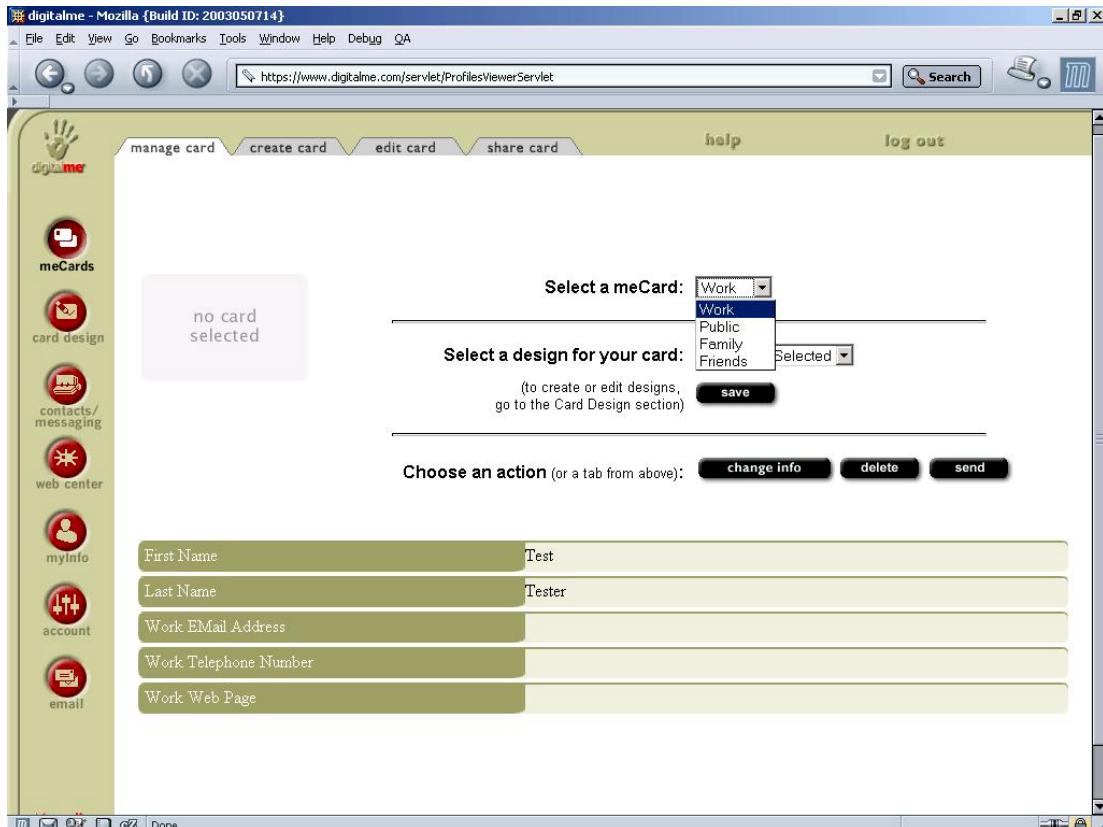
The "web center" allows the management of access data of web sites and of entries in web forms. The corresponding data are recorded via an additional application and remain available at Digitalme.

A connection to Liberty Alliance does not exist so far, although Novell is also active in the Liberty Alliance. Novell works on a solution for eDirectory, though, which is to be compatible with the Liberty-Alliance. This is to provide the user with the opportunity to exchange profile information within the circle of trust.

The standard vCARD, too, is not supported.

#### 4.2.4.2 Representation of Identities

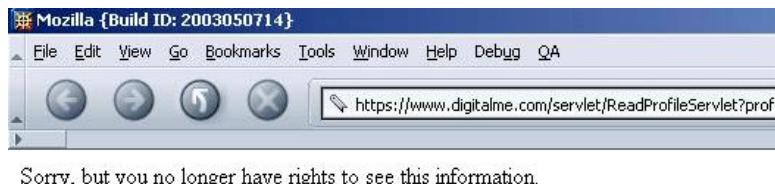
Identities are represented in the form of meCards which can be assigned to particular situations (e.g., Private, Work, Family) or chosen as free pseudonyms. The users are free to choose which data they would like to enter in these meCards and who is allowed to access them.



**Figure 50: Digitalme – User Can Choose a Situation for the meCard**

#### 4.2.4.3 Handling of Identities

The user can control how his personal information is shared and used. When he exchanges a meCard with a Digitalme member, he in essence gives them permission to use that information, and he can retract it.



**Figure 51: Digitalme – Visit to a Foreign meCard after Retraction of Permission**

#### **4.2.4.4 History Management**

The user can always view to whom the meCards have been sent or who has access to them. However, a history of the profile data used by the service cannot be viewed. The user can neither access information on the time at which a meCard or a form entry has been transferred nor on the time at which a page has been visited at the single sign-in service etc.

#### **4.2.4.5 Context Detection**

The user has to choose the deployment context of the meCards on his own. An automated identification is not planned. There is a special function for the categorisation of outside meCards.

#### **4.2.4.6 Rule Handling**

A rule handling function does not exist.

#### **4.2.4.7 Privacy Control Functionality**

The users are not specifically supported in asserting their privacy rights such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent. The users can define which meCard data can be viewed by which persons. This right can be withdrawn subsequently.

#### **4.2.4.8 Identity Recovery**

The restoration of an identity (meCard etc.) is not provided.

#### **4.2.4.9 Digital Evidence Functionality**

A digital evidence function is not provided by Digitalme.

#### **4.2.4.10 Categories**

#### **Usability – Perceived Usefulness**

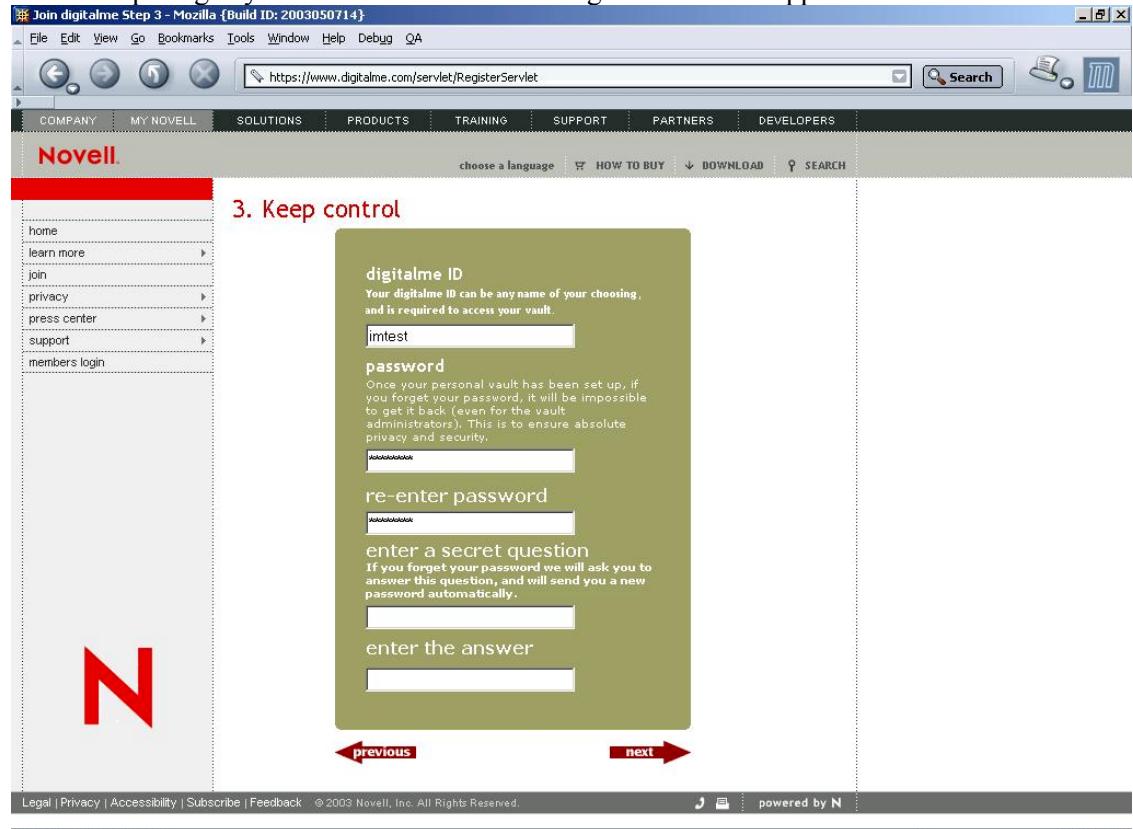
The single sign-in function and the form-fill-in function simplify the usage of web pages for the user. The authentication or form data have to be entered only once. The management and further usage is taken over by Digitalme. On the other hand, every usage of these functions requires a sign-in at Digitalme and the execution of the corresponding functions.

Rating:

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

### Usability – Perceived Ease of Use

The usage of Digitalme requires a registration by the user. During the registration process, some data such as the name, first name, e-mail address, password etc. are to be entered, and the design of the meCard has to be selected. After the data input, the account is activated immediately, without requiring any confirmation. The whole registration takes approx. 5 to 10 minutes.



**Figure 52: Digitalme – Register**

If the user wants to use the functions provided by Digitalme, he has to sign in first at [www.digitalme.com](http://www.digitalme.com) "members login" by use of the user name and password.

During this process, applets are loaded. Depending on the settings, the browser generally reports the installation of these applets to the user. Direct descriptions of the function of these applets or what happens if they are rejected will not be displayed. During the test phase, it occurred that if the answer to the question whether the applets were to be accepted or not was put aside (Internet Explorer 6.0) and another window was opened first, the browser could not be accessed anymore and it was impossible to get the query window back to the front again.

In order to store the access data for the single sign-in functions, the user has to click on "web center" and then select "Web Log in". Subsequently, the sites for which data have already been stored will be displayed. New sites can be added by selecting "Record". A special browser window will be opened in which the URL of the new site is to be entered and the normal authentication process is to be carried out. When Digitalme registers this, it asks if the data are to be stored and the sign-in process is continued. If the answer is positive, a corresponding entry appears in the "Web Log in". By highlighting this entry and clicking on "view", the site will be called up again and the sign-in process will be carried out automatically. Furthermore, the user can delete an entry in the "Web Log in" or view the stored data in plain text.

The auto-form-fill-in function works in a similar way. The user must have installed the appropriate toolbar which makes sure that the data can be stored in Digitalme when a form is filled in or a site is visited. These data can be used again and inserted automatically when the same or another site is visited once more.

---

**Rating:**

- The help function is not needed for standard activities: (+0.5)
- The manual is not needed for standard activities: (+0.5)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (+0.5)

**Usability – Malfunction Understanding**

The single sign-in function did not work with all tested pages. In most cases, the sign-in data were stored correctly and an automated sign-in was possible but, e.g., with ebay.com, however, this did not work. Digitalme recognised the data to be stored when recording the sign-in but an automatic sign-in was rejected, accompanied by an error message that said the user had not been recognised. Digitalme provided no reason for this, i.e., the user was unable to know what had gone wrong and how this error could be fixed.

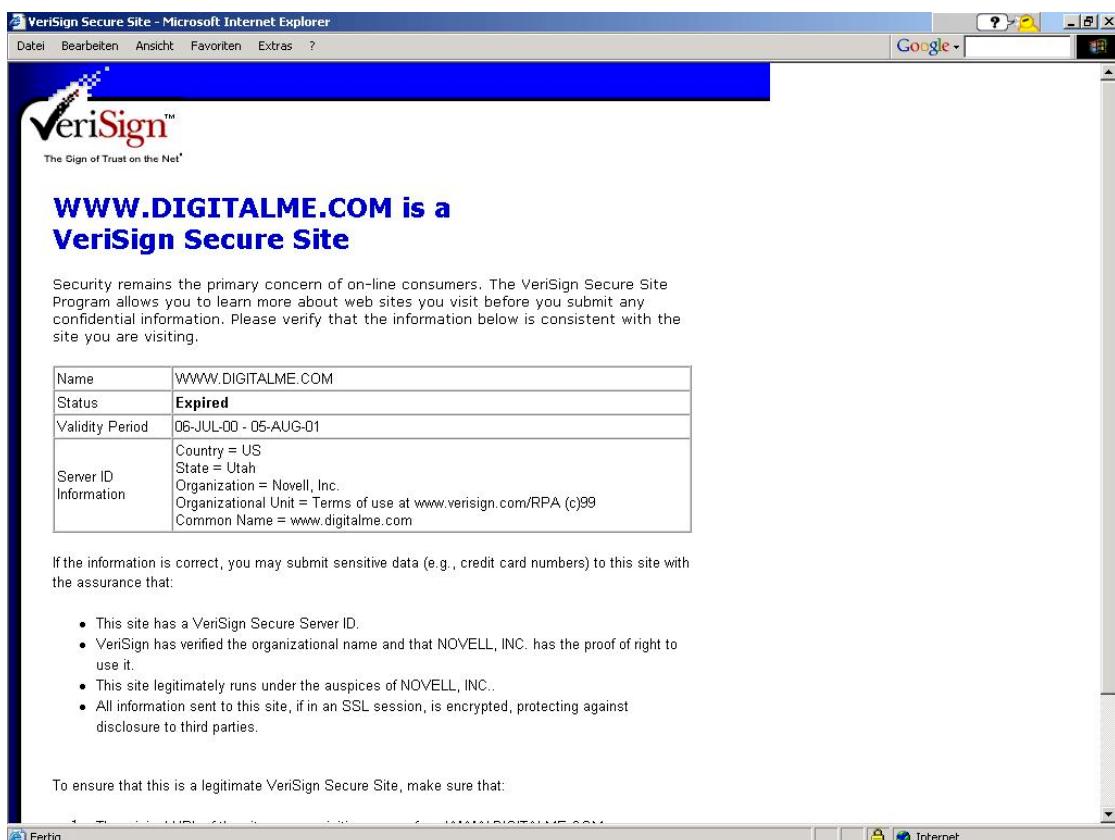
**Rating:**

- The user can recognise that an error occurred: (+1)
- There are suggestions for what to do next: (+1)

**Security – Confidentiality**

The registration process is secured by SSL with a key size of 128 Bit. This applies also for all data or cookies exchanged within the authentication process. At the sign-in, a certificate provided by Equifax is transferred and can either be accepted or rejected by the user.

The security of www.digitalme.com itself is confirmed by VeriSign. This implies that the site has a VeriSign Secure Server ID, VeriSign has verified the organisational name and that Novell, Inc. has the proof of right to use it, the site legitimately runs under the auspices of Novell, Inc. and all information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties. When the concerning certificate is called up via a click on the VeriSign button on the login page, though, the user is informed that the status was "Expired".



**Figure 53: Digitalme – VeriSign**

A security function provided by Digitalme is the auto-log out. According to the default setting, an automatic logout is carried out after 20 minutes.

This increases the security, particularly for the usage of Digitalme with computers that can be accessed by more than one user. After this period has run out, an access to Digitalme is impossible without another sign-in. However, in some cases, visited Digitalme pages remain accessible via the cache and the "back" function of the browser. Changes will be impossible, though. The user can define the number of minutes after which the logout is to be carried out. This function can also be switched off totally.

After the registration with Digitalme, the user can view all data of the auto-form-fill function and the single sign-in service in plain text. This includes the stored passwords too. If any one should be able to get illegal access to the Digitalme account, the intruder, to, would have access to all stored access data. Disfiguring at least the passwords would also be a protection from unwanted audience when using Digitalme who could read the plain text passwords, too. A warning that says that the passwords are displayed in a form that is readable for everyone is not provided.

### **Security – Integrity**

A unique ID which the user can choose guarantees integrity. If the user chooses an ID that is already in use, he will be asked to choose another one. The ID is not stored in encrypted form, though.

### **Security – Availability**

Digitalme is a server-based service. The responsibility for the availability is left to Novell. The extent of backups etc. is unknown.

---

### **Security – Rating**

- Transmitted data is encrypted: (by default: +2)
- Data access and manipulation is only possible after authentication: (by default: +2)
- Transmitted data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (by default: +2)
- IMA informs completely about all processed and transmitted personal data: (+1)

### **Privacy – User Empowerment**

The user can choose which information is to be included in the meCard which defines his digital identity. Furthermore, the user is notified about which personal data are stored for which purpose and to whom they are passed on. The profile data will only be passed on upon the user's request to do so. As far as the meCard is concerned, the user can also withdraw the right to view the meCard from selected receivers of these data.

P3P is not supported.

When using the single sign-in service, the sign-off from Digitalme does **not** mean the parallel sign-off from all sites authenticated via Digitalme. For this, a manual sign-off is required each.. Digitalme does not point out this circumstance explicitly, though.

### **Privacy – Transparency**

As said in the Novell Online Privacy Policy, if they change their information handling practices or other privacy aspects, they will post a prominent notice of their homepage those changes on this privacy statement, at least 30 days prior to their the implementation. The user will have a choice as to whether or not Novell uses their information in this different manner.

### **Privacy – Data Minimisation**

Data minimisation – reduction of processed personal data; use of pseudonyms / anonymity; unlinkability – is not in the focus of this IMA.. During the registration process, Digitalme asks for the first name, last name and e-mail address. Furthermore, an ID, a password and a secret question plus the answer (which can all be chosen at will) have to be entered. For the usage of the service, neither the first name nor the last name nor the e-mail address are definitely necessary.

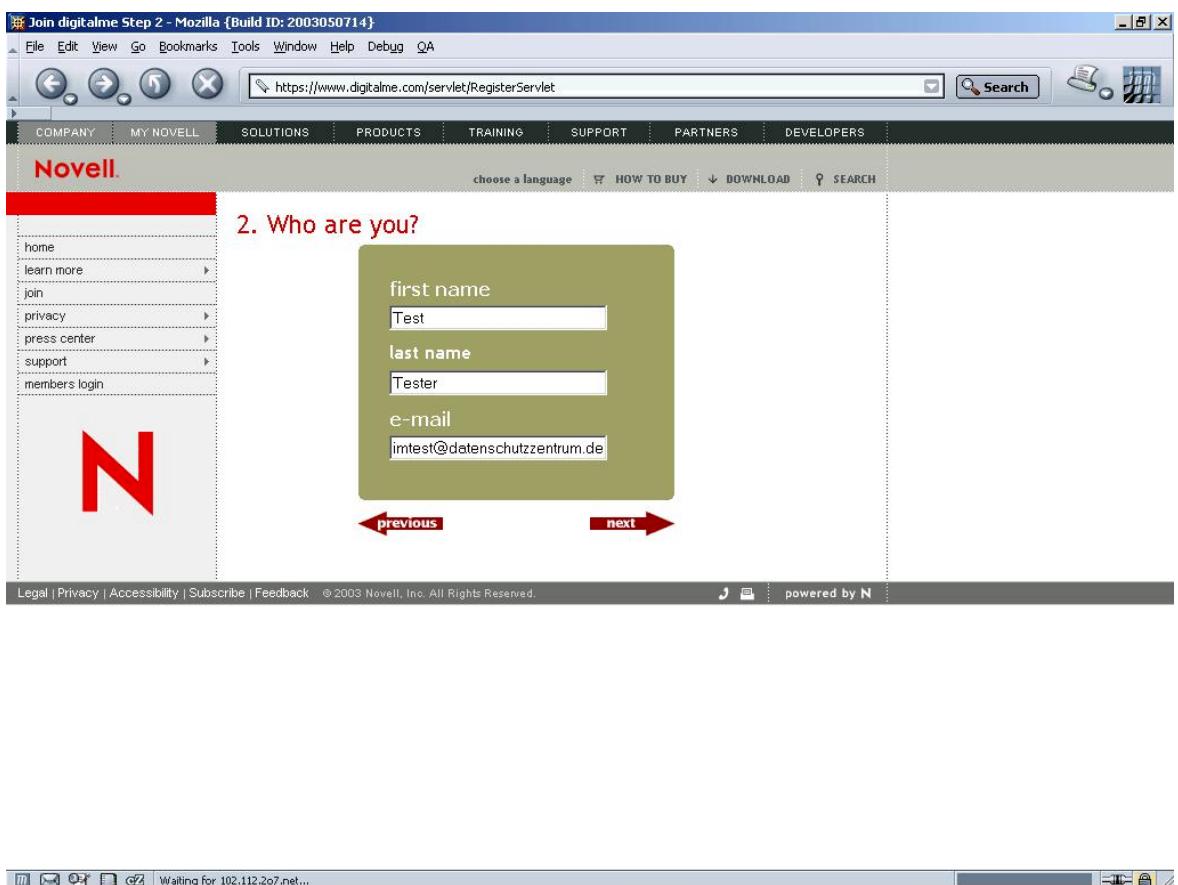


Figure 54: Digitalme – "Who are you?"

### Privacy – Rating

- There is a privacy policy: (+1)
- Privacy issues (law etc.) are documented: (+1)
- The user has freedom of choices concerning the identity management: (+1)
- The user is supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent: (+1)
- The IMA informs user about purpose of data processing or does not process personal data: (+1)
- The IMA informs completely about all used and transmitted personal data: (+2)
- Usage of pseudonyms / anonymity is possible: (+1)
- Usage of different pseudonyms is supported (+1)

### Law Enforcement and Liability

The functions of Digitalme do not support expressly law enforcement or liability. However, it is at least a technical circumstance that user data and sometimes probably temporary usage data are stored on the servers Digitalme. These data could be accessed by law enforcement agencies.

Rating:

- There is a log function: (+1)

### Trustworthiness – Multilateral Security

Multilateral security is not sufficiently supported. There is no advanced documentation of the deployed mechanisms and protocols. The system is completely owned and controlled by the Novell company. the existence of further security systems is unknown.

---

### **Trustworthiness – Seals**

The adherence to the Privacy Policy is controlled by Online Privacy Alliance, Direct Marketing Association and TRUSTe.

### **Trustworthiness – Rating**

- The IMA provider is an established company being well observed: (+1)

#### **4.2.4.11 Platform and Environment**

##### **Hardware, Software, Services**

Depending in the way Digitalme is used, there are different requirements to the deployed browser. For the usage of the single sign-in service, the Internet Explorer or Netscape Navigator 4.0 or higher or a compatible browser is required. The auto-form-fill function requires the installation of a browser toolbar which again requires the Internet Explorer 4 / 5 or Netscape Navigator 4. Mozilla 1.4 was not recognised by the toolbar. Explorer 6.0 had problems, too.. Only a grey surface appeared, without any recognisable functions.

##### **Installation, Maintenance, Use**

The usage of Digitalme requires the registration via the page [www.digitalme.com](http://www.digitalme.com) as described above.

The installation of the browser toolbar requires its download first. The downloaded file has to be executed to trigger the automatic installation and appearance of the toolbar in the status line of the browser (if there is one). The registration takes about 5 minutes, the installation of the toolbar takes about one minute after the download. Depending on the previous knowledge, understanding the advances functions takes approx. one hour. The time for the further set-up of these functions (e.g., further meCards depends on the user's requirements.

##### **Technical Resource Requirements**

Digitalme can be used by a single person. The system is operated on an external server of the Novell company. The usage is free.

##### **Availability**

Digitalme is distributed. In an initial test in January 2003, the sign-in page of Digitalme could not be accessed. The same result appeared on a visit at the Novell booth at the CeBIT exhibition in Hanover in February 2003 and was explained by the present Novell employees who said that this system was only supported by a single person in the company and that it was a pilot system to show the deployment options of identity management products by Novell. In May 2003, a registration was possible without problems. During the subsequent test period that lasted until June 2003, there were no downtimes noticed; the service was fully available.

##### **Installation Base IMS**

The number of users of Digitalme is unknown.

##### **Interoperability / Standards**

Digitalme is a server-based system that deploys its own techniques. Standards such as "vCARD" are not supported.

### Guarantee for Trustworthiness

Novell has adopted leading industry privacy practices as set forth by the Online Privacy Alliance, Direct Marketing Association, and TRUSTe. Furthermore, Novell is a member of the Liberty Alliance. Further monitoring of Digitalme are not known.

### Legal and Contractual Framework

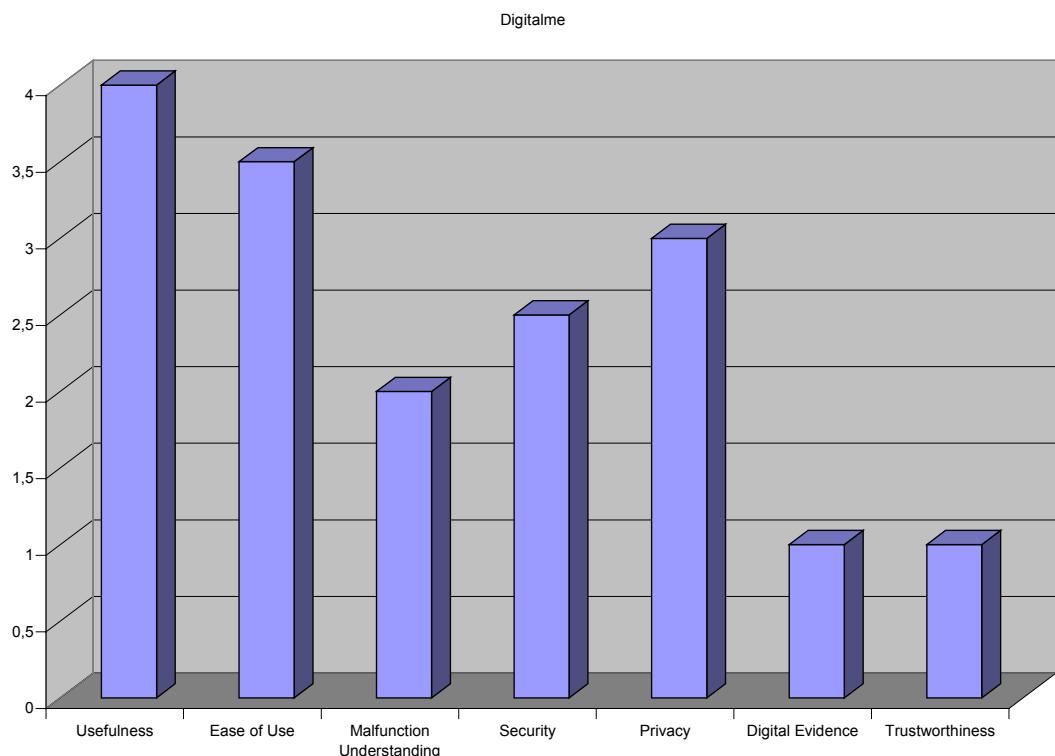
Novell is a world-wide operating US-company. Digitalme is operated on US-American servers. The service addresses users outside the US, i.e., that depending on the circumstances, other countries' laws may apply in single cases.

### Nature of Provider

Novell is an incorporation.

#### **4.2.4.12 Conclusion**

The following chart shows the main evaluation results of Digitalme normalised to 5 points maximum:



**Figure 55: Overview Evaluation Digitalme**

## 4.2.5 Yodlee

Yodlee idea of its e-personalisation solution is to offer consumers the facility of one-click access to all their personal on-line accounts. Yodlee wants to simplify the administration of web accounts, at banks, e-mail services, news services and other providers. Unified on one page, personal data can be queried and passwords can be managed.

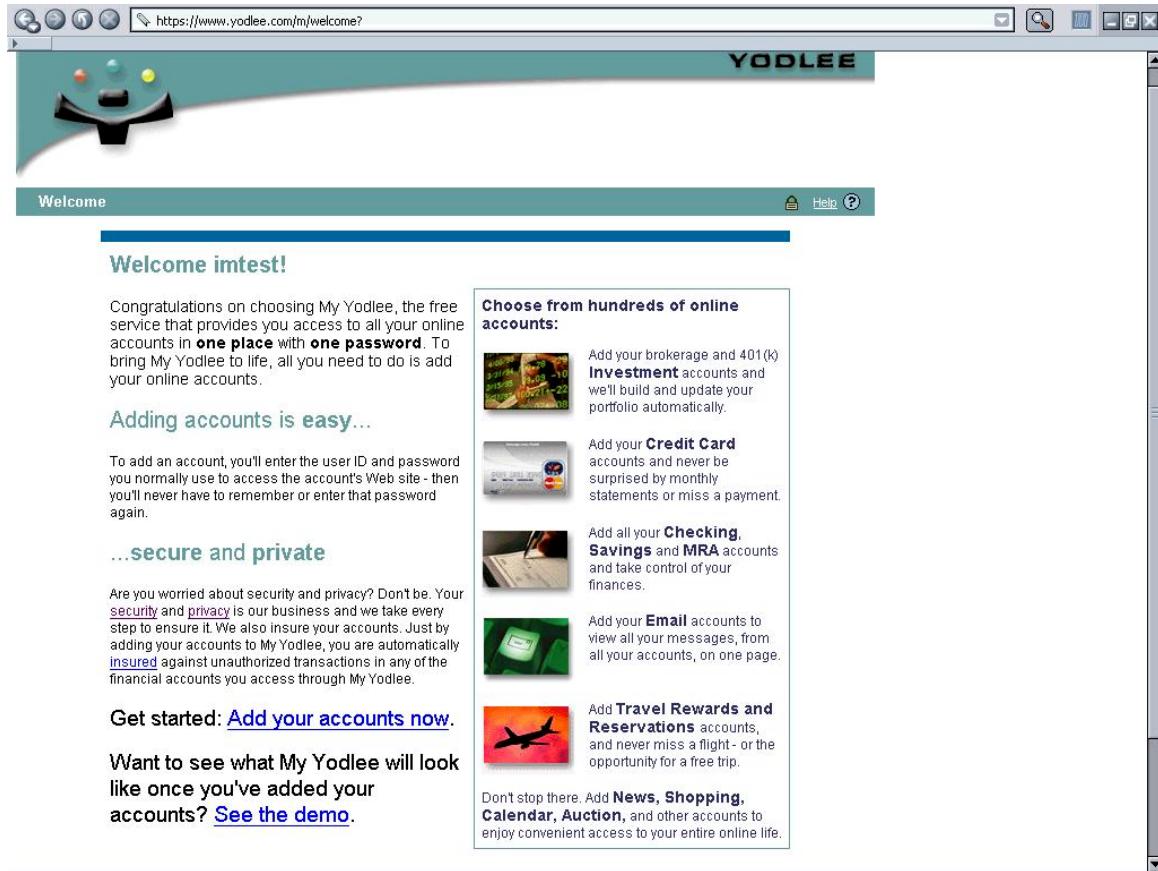


Figure 56: Yodlee – Welcome

The internet accounts can be accessed via web (My Yodlee), PDAs (Yodlee2Go) and Internet-capable mobile phones. A software development kit for the development of new applications is provided<sup>172</sup>.

It is possible to let Yodlee send alerts to the cellular phone, e-mail or pager of the user. The Alerts feature lets the user configure self-addressed, automated messages that provide updated account information for Banking, Investment, and Credit Card accounts. Once a device/destination has been set up, the user can create alerts for individual Banking, Investment, and Credit Card accounts on the respective "Edit Account Settings" page. He can choose from three types of Alerts: "Due Date Alerts" are sent a set number of days before the payment due date; "Threshold Alerts" are triggered when a balance goes above or below a set amount; "Scheduled Alerts" are sent on a daily, weekly, or monthly basis.

### 4.2.5.1 IMS Category: Operational Area, Purposes and Functions/Interfaces

Yodlee serves the administration of various accounts, e.g., concerning e-mail, credit cards, airlines, banking, travel and investment.

Yodlee enables users to:

<sup>172</sup> <https://www.yodlee.com/solutions/>.

1. Create a hub for personal information from key websites and services.
2. View updated snapshots of all recent account activities in one central place.
3. Access all personal accounts across the web with a single click, eliminating the need to remember multiple passwords.
4. Register for new services and accounts quickly and easily using pre-filled forms.
5. Access and synchronise personal information with handheld devices and web-enabled phones<sup>173</sup>.

The Yodlee e-personalisation platform represents the basis for applications with the personal data and is divided into two components:

1. The Yodlee e-personalisation engine is responsible for the data maintenance and data composition of this information.
2. The Yodlee dissemination engine is responsible for the secure communication of the personal data between different accounts, services, platforms and devices.

#### **4.2.5.2 Representation of Identities**

Yodlee manages different kinds of extant accounts within a single administration and user interface. These accounts can be, e.g., e-mail accounts, credit cards, airlines, banking and investments etc. It is possible to create a "Custom Account" for accounts the user cannot access via the Internet, for personal property such as jewellery or real estate, or if he wants to create a bookmark link. The registration with Yodlee can be done by use of a pseudonym chosen by the user.

#### **4.2.5.3 Handling of Identities**

The user can choose his "Yodlee ID" on his own. Further on, the user can define which accounts at which companies are to be managed by Yodlee.

#### **4.2.5.4 History Management**

Yodlee provides grouped information about the activities on bank accounts if the bank supports the Yodlee service.

#### **4.2.5.5 Context Detection / Rule Handling**

The user has to choose by himself which accounts Yodlee is to manage and which functions are to be executed. There will be no context detection; a rule handling is impossible.

#### **4.2.5.6 Privacy Control Functionality**

The users are not specifically supported in asserting their privacy rights such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent. The users can choose if they want to log into their on-line accounts without re-entering the user names and passwords.

#### **4.2.5.7 Identity Recovery**

There is no identity recovery function of Yodlee.

#### **4.2.5.8 Digital Evidence Functionality**

A digital evidence functionality is not provided.

---

<sup>173</sup> <https://www.yodlee.com/solutions/yodleeforweb.html>.

## 4.2.5.9 Categories

### Usability – Perceived Usefulness

Yodlee gives the user a complete overview of his accounts. After the accounts have been registered, it is unnecessary to sign in manually at every single account. By this, Yodlee accelerates the management of different accounts.

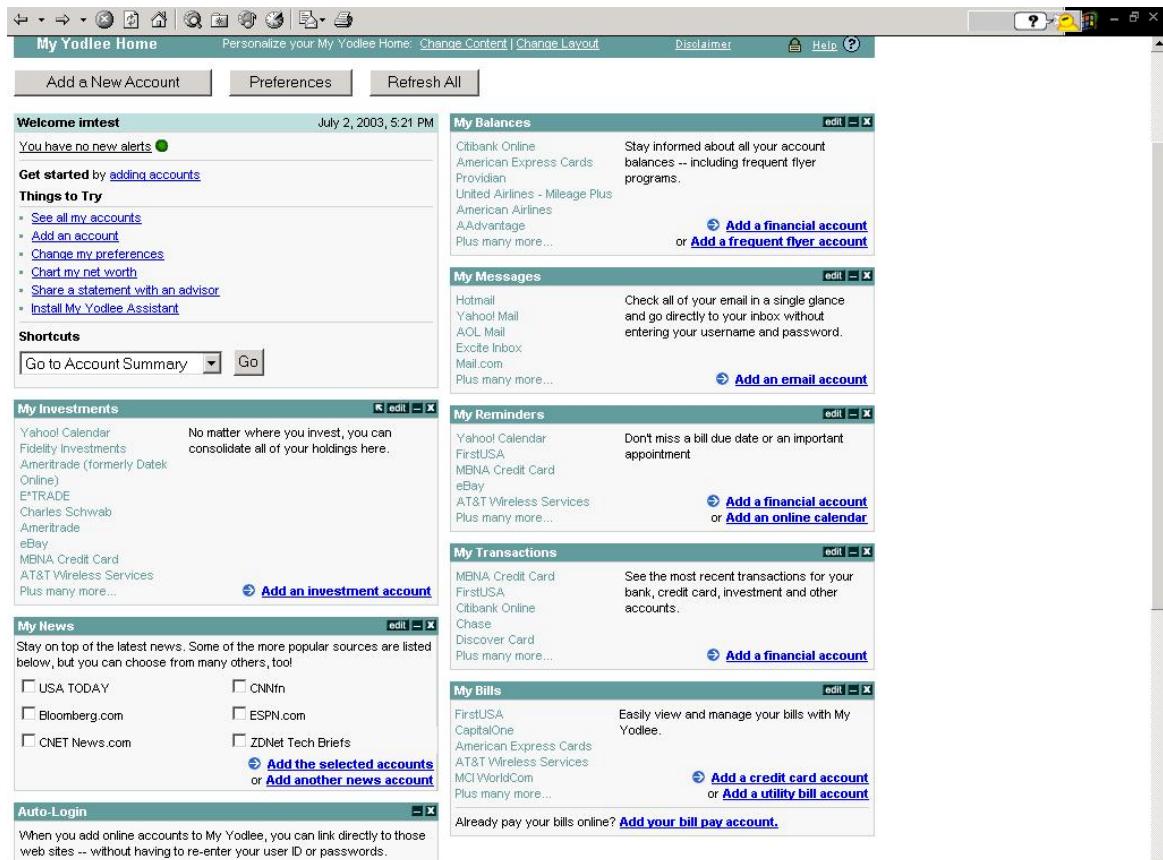


Figure 57: Yodlee – Accounts

The alert-functionality helps the user to remember special dates or events in connection with his accounts and gives him the possibility of a faster reaction.

These functions of Yodlee, however, will only work if the corresponding external accounts are supported by Yodlee. Lists of the usable accounts can be viewed on the Yodlee internet page and include American and British institutes and companies in particular. As far as the e-mail addresses are concerned, at least important e-mail providers of the central European area such as gmx.com or web.de are missing. For these non-supported accounts, a separated sign-in procedure is still required.

Rating:

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

### **Usability – Perceived Ease of Use**

The user can choose the accounts he owns and wants to manage via Yodlee from a list provided by Yodlee. Subsequently, he is asked to enter the appropriate access data. This process is simple and quickly done if the appropriate data are given.

The additional application "My Yodlee Assistant" can help the user to add his accounts at other web sites to his Yodlee account. When the user logs to a web site that is supported the "My Yodlee Assistant" will pop up and ask if the user wants to add it to the Yodlee account.

The installation of the "My Yodlee Assistant" requires the Microsoft Internet Explorer version 5 or higher and calling up the installation page. After the selection of the corresponding option, the installation procedure is carried out automatically. Only a popup window of the Microsoft Internet Explorers referring to the application installation has to be answered with "Yes".

The My Yodlee Assistant pop-up shall automatically appear when the user logs in to a web site supported by Yodlee. If the site the user is logging into is owned by a company that owns other on-line services, those services will appear in a menu. The user has to select the sites he wants to add to his Yodlee account. If this menu doesn't appear, this means that the site is not owned by a parent company with other web sites.

The user has to enter his User ID and password to the Yodlee service and not the web site he just logged into. At least he has to press "Add Now".

Rating:

- The help function is not needed for standard activities: (+0.5)
- The manual is not needed for standard activities: (+0.5)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (+0.5)

### **Usability – Malfunction Understanding**

Yodlee has an extensive help dashboard and help index about the main topics of the system.

Rating:

- The user can recognise that an error occurred: (+1)
- In case of a malfunction the function presents a complete and understandable description of the error: (+2)
- There are suggestions for what to do next: (+1)

### **Security – Confidentiality**

As Yodlee says, password and account data are stored and transmitted in encrypted format at all times. All data is securely housed in the "Exodus Vault", an Internet server hosting space that provides enhanced physical security, fire protection and electronic shielding<sup>174</sup>.

Personal information is entered through Secure Socket Layer (SSL), which creates an encrypted connection between the browser of the user and the servers of Yodlee.

At the registration, My Yodlee permits passwords with a minimum length of 6 characters which include at least one symbol or number. This increases the security against unwanted access by third parties who try to find out the passwords.

---

<sup>174</sup> <https://www.yodlee.com/policy/security.html>.

---

### **Security – Integrity**

As Yodlee says a Network-based IDS (intrusion detection system) provides 24x7 network monitoring and alerts security personnel to any external attacks on the network. Multiple layers of firewalls are used to guard against unauthorised access to the network.

### **Security – Availability**

Security personnel monitor the system 7 days a week, 24 hours a day. Access to servers requires multiple levels of authentication, including biometrics (hand print scan) procedures.<sup>175</sup>

### **Security – Rating**

- The stored data is encrypted: (by default: +2)
- Transmitted data is encrypted: (by default: +2)
- Data access and manipulation is only possible after authentication: (by default: +2)
- Transmitted data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (by default: +2)
- Fall-back solutions and / or external services for security are provided: (+1)
- IMA informs completely about all processed and transmitted personal data: (+1)

### **Privacy – User Empowerment**

The user can choose which accounts are to be managed via Yodlee. Furthermore, the user can decide if he wants to log into her/his on-line accounts without re-entering the user name and password. This is the default setting as well as the setting that Yodlee sends a personalised statement of accounts of the user to his trusted advisor.

### **Privacy – Transparency**

Yodlee provides the user with a Privacy Policy in the P3P format and a Security Policy. Yodlee promises to not passing on any user data to third parties and to not contacting the user without being asked to.

The privacy protection practices of the My Yodlee service are checked by the organisations TRUSTe, BBBOnLine and VeriSign.

However, if services are provided by partner companies, their privacy protection practices are to be considered, which is explicitly pointed out by Yodlee in its Privacy Policy<sup>176</sup>. The user is still not able to see, though, if a service is provided directly by Yodlee or by one of the partners.

### **Privacy – Data Minimisation**

Data minimisation – reduction of processed personal data; use of pseudonyms / anonymity; unlinkability – is not in the focus of this IMA.. The registration only requires an ID which the user can choose freely, the password and an e-mail address. Further personalised information like the postal code are optional, which the registration page shows explicitly to the user.

---

<sup>175</sup> <https://www.yodlee.com/policy/security.html>.

<sup>176</sup> <https://www.yodlee.com/policy/privacy.html#q7>.

**Important Notice:** In compliance with the Children's Online Privacy Protection Act of 1998 (COPPA), Yodlee does not accept membership registrations from users who are under 13 years of age. For more detailed information, please refer to our [Terms and Conditions](#).

**Sign-In Information**

Please choose a My Yodlee ID and password.

My Yodlee ID:

My Yodlee password:

**Must** be between 6-50 characters  
**Must** contain at least one number  
**Must** contain at least one letter

Verify password:

E-mail address:

**Personalization Information (Optional)**

At Yodlee we value your privacy and guarantee to adhere to the policies of TRUSTe.

Postal / Zip code:

I would like to receive occasional e-mail updates of new features, surveys and special offers from Yodlee.

**Continue**

**REVIEWED BY**  
**TRUSTe**  
Site privacy statement

**VeriSign**

**Figure 58: Yodlee – Sign In**

### **Privacy – Rating**

- There is a privacy policy: (+1)
- Privacy issues (law etc.) are documented: (+1)
- The user has freedom of choices concerning the identity management: (+1)
- The IMA informs user about purpose of data processing or does not process personal data: (+1)
- User is only asked for needed data overall: (+1)

### **Law Enforcement and Liability**

The Functions of Yodlee do not support law enforcement and liability. However, it is at least a technical circumstance that user data and sometimes probably temporary usage data are stored on the servers of Yodlee. These data could be accessed by law enforcement agencies.

Rating: 0 Points

### **Trustworthiness – Multilateral Security**

Multilateral security is not sufficiently supported. Yodlee is a server-based system operated by Yodlee Inc.. The deployed systems and techniques are not documented completely. About a segregation of power nothing is known.

### **Trustworthiness – Seals**

The site of Yodlee has a VeriSign Secure Server ID. TRUSTe and BBBOnLine control the privacy policy of the site, but there are no further seals.

---

### **Trustworthiness – Rating**

- The IMA provider provides a federation of independent companies: (+1)

#### **4.2.5.10 Platform and Environment**

##### **Hardware, Software, Services**

The usage of Yodlee requires a current browser. If the "My Yodlee Assistant" is to be deployed, the MS Internet Explorer 5 or higher is required.

##### **Installation, Maintenance, Use**

The usage of Yodlee requires the user registration at [www.yodlee.com](http://www.yodlee.com) as described above.

Afterwards, the required accounts can be embedded. The registration takes a few minutes. The embedding of the individual accounts can be carried out similarly quickly if the required access data are given.

##### **Technical Resource Requirements**

Yodlee can be used by a single person. It is operated on an external server of Yodlee Inc. The usage is free.

##### **Availability**

During the test phase in June 2003, no downtimes were noticed.

##### **Installation Base IMS**

According to the web site of Yodlee it offers the customers access to a dynamic summary of personal account information from a growing list of over 6,100 sites<sup>177</sup>. Other sources report approx. 2,000 sites<sup>178</sup>. Content partners are, e.g., Quicken.com, Paytrust, WeddingChannel.com, MSNBC.com, FreeAgent.com, PayPal etc<sup>179</sup>. Others are Yodlee Co-Brand Clients that licence Yodlee e-personalisation technology for their own website like Yahoo!, American Express, HSBC, Palm and AOL.

##### **Interoperability / Standards**

Among others, the data formats HTML, XML, OFX (Open Financial Exchange Format of Microsoft Money), QIF (Quicken Interchange Format) are supported. During the registration and authentication processes and when new accounts are added and used, cookies are deployed. The transmission is carried out via SSL. For the data transfer, 128 bit RC4 and 3DES are deployed in connection with SSL.

##### **Guarantee for Trustworthiness**

My Yodlee provides free fraud insurance which, in the event that unauthorised on-line transactions occur with any of users' My Yodlee accounts, the user covered up to \$ 100,000 of the loss for which he'd otherwise be responsible for under Federal Banking Regulations<sup>180</sup>.

---

<sup>177</sup> <https://www.yodlee.com/solutions/>.

<sup>178</sup> <https://www.yodlee.com/solutions/yodleeforweb.html>.

<sup>179</sup> <https://www.yodlee.com/partner/>.

<sup>180</sup> <https://www.yodlee.com/policy/security.html#q6>.

### Legal and Contractual Framework

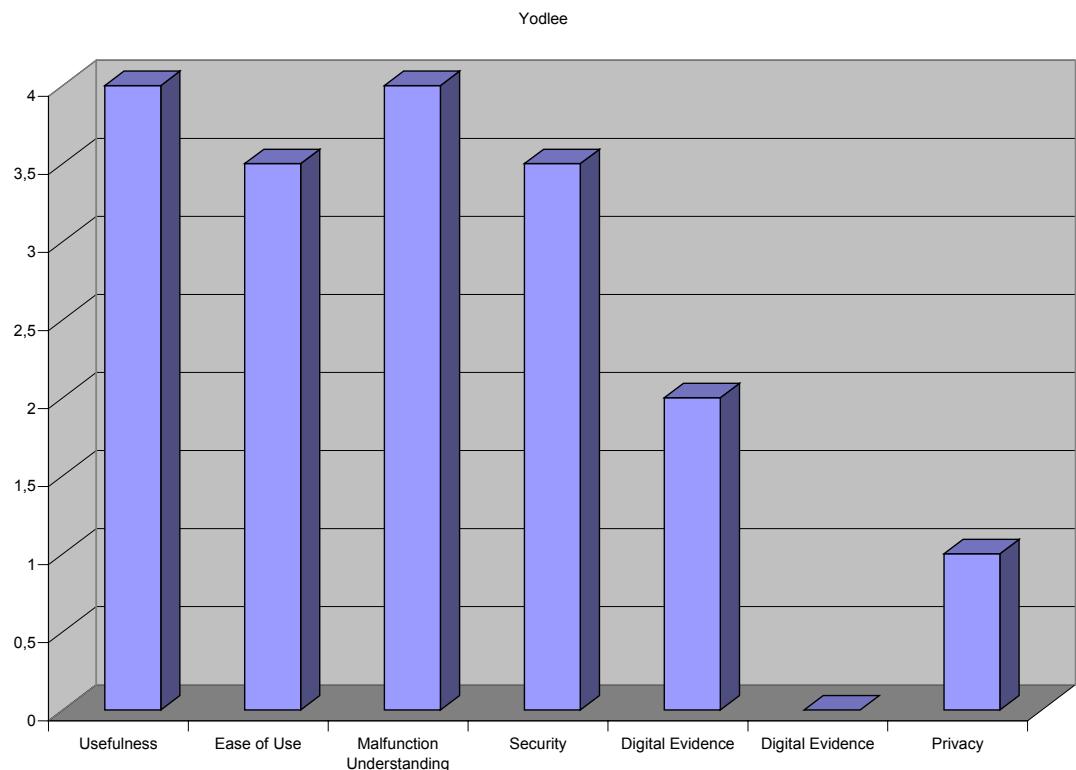
Yodlee Inc. Headquarters are domiciled in North America, Redwood City (CA). They have offices in Atlanta, London (United Kingdom) and Bangalore (India). The main used law system should be anglo-american.

### Nature of Provider

Yodlee is an Incorporation.

#### **4.2.5.11 Conclusion**

The following chart shows the main evaluation results of Yodlee normalised to 5 points maximum:



**Figure 59: Overview Evaluation Yodlee**

## **4.2.6 Microsoft Outlook Express 6 SP1**

Outlook Express 6 SP1 (short Outlook Express) is an e-mail client provided by Microsoft. It is delivered along with the current version of Windows XP (XP, Windows 2000) or can be obtained as apart of the Microsoft Internet Explorer package, e.g., via [www.microsoft.com](http://www.microsoft.com). It enables the reception, display, creation and administration of e-mails via POP3, IMAP or HTTP. This view of Outlook Express refers to its identity management functions.

### **4.2.6.1 IMS Category: Operational Area, Purposes and Functions/Interfaces**

Outlook Express can be deployed for various types of e-mails and is able to interpret the most usual formats of attachments (e.g., UUENCODE/MIME). The user can set up different separate identities within which the mail account settings and program settings can be stored and called up. Furthermore, it is possible to set up various accounts which can address different mailbox servers / accounts within a single identity.

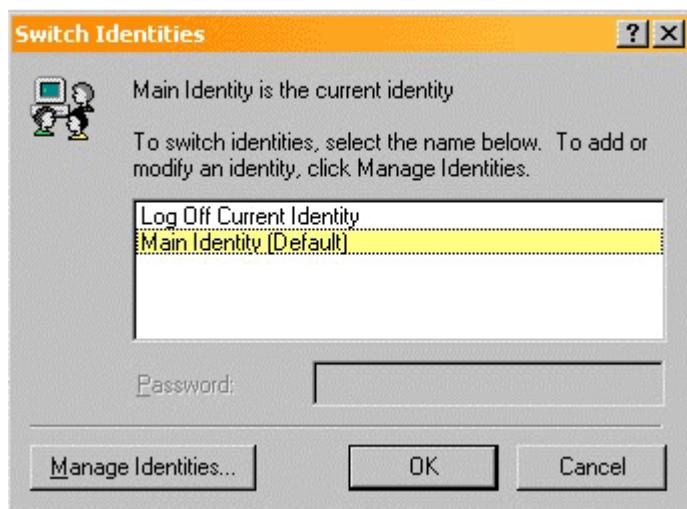
Outlook Express offers the opportunity to embed other programs such as PGP.

### **4.2.6.2 Representation of Identities**

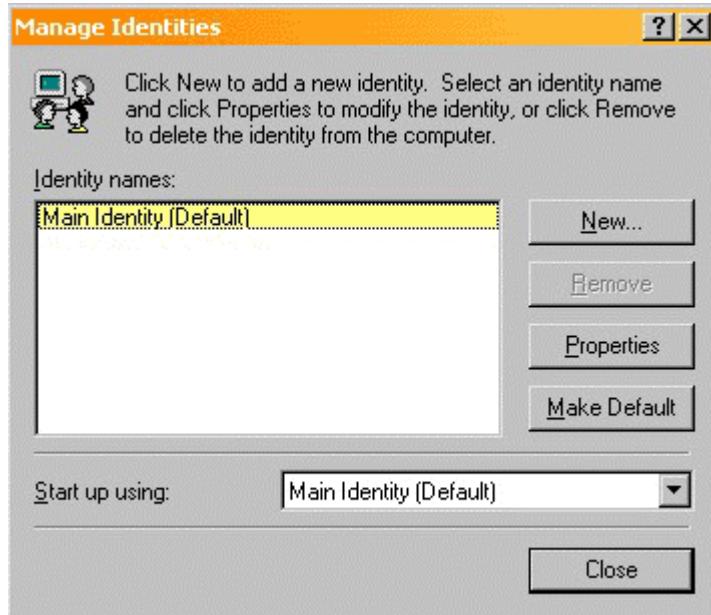
The identities are to be created and named by the user himself. The identity name can be chosen at will and does not have to be equivalent to the real user name. The data of the e-mail accounts (e-mail address, server, username, password) connected with the corresponding identity have to be entered according to the technical statements by the corresponding e-mail provider. Depending on the provider type, the e-mail account data such as the e-mail address and related person can be created within a domain freely or only after an identity check. However, the name of the sender which is displayed in the header of the e-mail and the reply address can be chosen at will.

### **4.2.6.3 Handling of Identities**

The user can create, delete or maintain / modify identities. The data to be entered can be the identity name and (upon wish) a password. Further on, the user can switch over between the different identities.



**Figure 60: Outlook Express – Switch of Identities**



**Figure 61: Outlook Express – Management of Identities**

#### 4.2.6.4 History Management

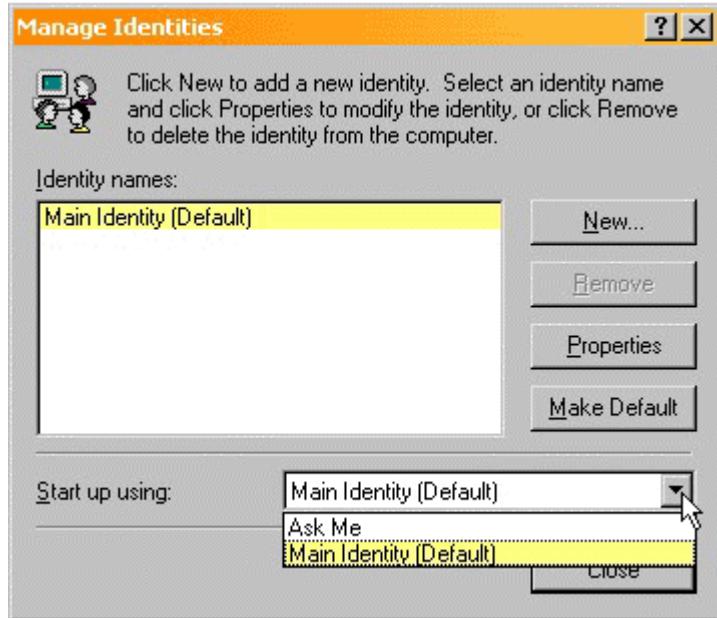
An explicit history function is not provided. Outlook Express does not register when and which identity was activated nor when the server has been checked for e-mails within this identity. When a new mail is created, however, it is provided with the current time and is first stored in the "out" folder. After having been sent, it can be viewed including the date in the "sent" folder.

#### 4.2.6.5 Context Detection

The user has to select the required identity manually. There is some kind of context detection function which however, is limited to the automatic insertion of the account address to which the e-mail has been sent when the user replies directly to an e-mail he received. This detection refers to the case that a user maintains several accounts with different account data within one identity.

#### 4.2.6.6 Rule Handling

For the identity switch, there is no possibility to adjust the rules. The user can only define which identity is to be used as the standard identity and via which account the e-mail traffic is to take place by default.



**Figure 62: Outlook Express – "Which Identity?"**

#### 4.2.6.7 Privacy Control Functionality

The users are not specifically supported in asserting their privacy rights such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent.

Outlook Express 6 offers the option to assign a password (which can be chosen at will) to each identity. When changing the identity, the user has to enter the password assigned to this identity. Further on, the users can define that the e-mails in the folders can be deleted manually to prevent others from subsequently fathoming the e-mail traffic by use of the settings within an identity in Outlook Express.

Further on, Outlook Express offers the option to sign and / or encrypt e-mails. Outlook Express can embed corresponding certificates for this purpose. In this context, Microsoft provides hints on its web pages on where appropriate digital IDs are available and mentions Verisign Inc., GlobalSign, British Telecommunications and Thawte Certification<sup>181</sup>. The link to Verisign Inc. did not work at the time of the test, though. The selection of "Call ID..." within the default settings of Outlook Express only lead to an overview page about the security features of Microsoft Internet Explorer.

#### 4.2.6.8 Identity Recovery

If an account or identity are deleted, a restoration is impossible.

#### 4.2.6.9 Digital Evidence Functionality

There is no digital evidence functionality at Outlook Express 6 for the user.

#### 4.2.6.10 Categories

#### Usability – Perceived Usefulness

The usage of different identities simplifies the administration of different e-mail accounts. Although it is also possible to manage the different accounts within one identity, this may

<sup>181</sup> <http://office.microsoft.com/assistance/2000/certpage.aspx?&helpid=1033&path=outldigid.asp>.

probably require an increase of attention concerning the corresponding settings such as the sender address etc. if there are many different accounts. With the identity management, in contrast, the accounts can be grouped, e.g., by particular situations (private, job) or users of this computer (e.g., family members). The user can then configure Outlook Express according to the individual requirements of each identity.

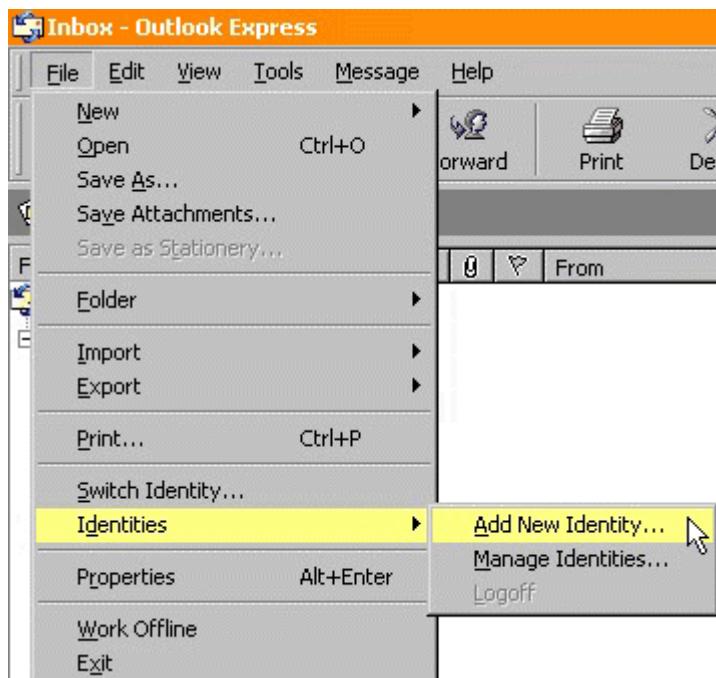
For (private) persons who have only one or two different e-mail accounts, this function hardly makes sense, though.

Rating:

- Application benefits usage several times a month: (+1)
- Time for first time adjustment is less than time for action without IMA: (partly +0.5)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

### **Usability – Perceived Ease of Use**

The effort of using the identity management function of Outlook Express is low. A new identity can be created by selecting File / Identities / Add new identity.



**Figure 63: Outlook Express – "Add New Identity"**

Only the name of the new identity has to be entered. After this, Outlook Express asks if the user wants to switch to the new identity. When the user clicks on "Yes", he is registered under the new identity and can configure the dedicated accounts for e-mail and news. For switching identities the user has only to select File / Switch Identity and to choose the identity he wants to use from a list.

Rating:

- The help function is not needed for standard activities: (+0.5)
- The manual is not needed for standard activities: (+0.5)
- Help function, manual and support are not needed at all: (+1)
- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)
- A complete and understandable help function is provided: (+0.5)

---

## **Usability – Malfunction Understanding**

The identity management functions are explained step by step in the help file of Outlook Express. If further problems occur, the user may find more help on the Product Support Server Web site with the Knowledge Base of Microsoft. Some problems with the usage of different identities are explained there after Outlook Express as the product and "Identity" as the match code are entered. The web site is structured in a quite complicated way, though, and is intended for all Microsoft products, i.e., finding the required information might become a tough procedure for an inexperienced user.

Malfunctions have not been noticed within the test period.

Rating:

- The user can recognise that an error occurred: (+1)
- In case of a malfunction the function presents a complete and understandable description of the error: (+2)
- There are suggestions for what to do next: (+1)
- The function makes a sensible suggestion about what to do next: (+1)

## **Security – Confidentiality**

The selection of an identity can be coupled with a required password input. This does not prevent, however, that the data can be viewed by everyone who has access to the relevant files on this computer. The e-mail folders are stored in plain text in the subdirectories and can be read by use of text viewing applications. It is also possible to read or edit e-mails by copying the mail folder files from one identity to another.

The security risks of Outlook Express consist particularly in the download and display of e-mails with content beyond the normal text or active content (ActiveX, HTML, JavaScript etc). In the past, there were often problems concerning the security of Outlook Express. Since the SP1 for Outlook Express 6, at least attachments that could contain viruses according to Outlook Express' opinion cannot be displayed (e.g., Microsoft Word files) by default anymore. The option to display of text contents only has to be activated by the user, though.

## **Security – Integrity**

Regarding the circumstance described above that the mail folders are given in plain text, it is also possible to manipulate these data. A simple data modification by use of an editor was recognised by Outlook Express, and the modified e-mail was not displayed anymore. A notification about the manipulation is not provided, though. However, it would not be difficult for a hacker to adjust the corresponding checksums in order to infiltrate a manipulated e-mail. This would only be possible with an access to the computer of the user, though. Optionally it is possible that Outlook Express encrypts the e-mail folders. But this is no default setting.

## **Security – Availability**

Outlook Express does not provide a possibility to back up the identity data. Only the messages and address books can be exported and read in again later. A complete backup requires the manual storage of the directories in which Outlook Express keeps the user data. This is made difficult, however, by the fact that, depending on the deployed MS Windows version, Outlook Express uses different directories for the data storage which are not clearly recognisable immediately.

## **Security – Rating**

- The stored data is encrypted: (optional: +1)
- Transmitted data is encrypted: (optional: +1)

- Data access and manipulation is only possible after authentication: (optional: +1)
- There are known bugs which could be security-relevant: (-2)
- There are patches / revisions (+1)
- Stored data is signed with digital signature or comparable mechanism to prevent undetectable manipulation: (partly by default: +1)
- Backup & restore of data is supported: (partly +0.5)
- Backup & restore of data is (manually) possible with adequate effort: (partly +0.5)

### **Privacy – User Empowerment**

The identity function of Outlook Express does not transmit any personal data to the outside but represents an administration option on the client side only.

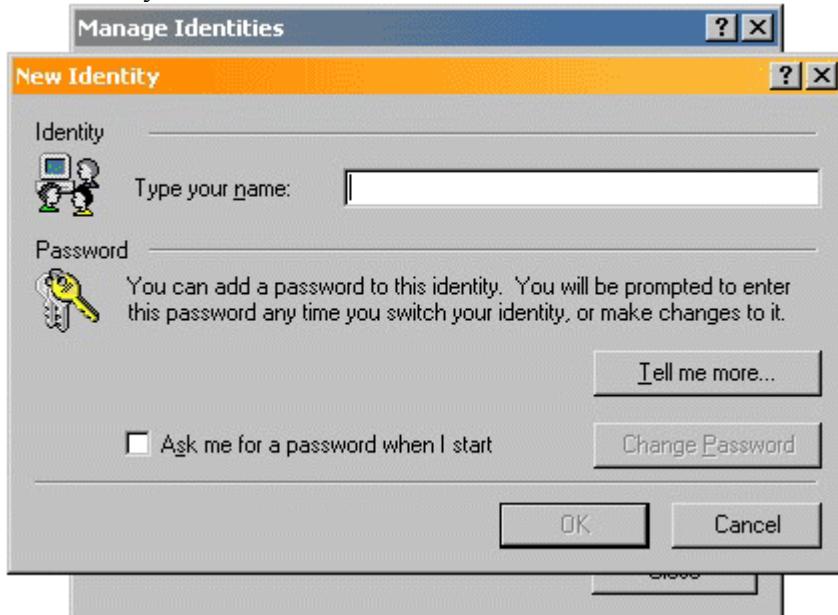
A privacy problem can appear with Outlook Express if e-mails are displayed that contain HTML code or other contents beyond plain text. By these, automatic reading confirmations can be generated via the download of, e.g., images or web bugs. The mail sender receives the IP address of the mail recipient and other data such as a referrer. The display of HTML could only be prevented by switching off the preview function of Outlook Express prior to the SP1. The current version provides the opportunity to view plain text only. This has to be activated by the user, though.

### **Privacy – Transparency**

The name of the selected identity is displayed both in the top line of the program and below the selection buttons. At the program start, the identity to be used is queried if the user has not adjusted the settings to define a standard identity.

### **Privacy – Data Minimisation**

Data minimisation – reduction of processed personal data; use of pseudonyms / anonymity; unlinkability – is not in the focus of this IMA.. The identity management only requires the input of a name for the identity.



**Figure 64: Outlook Express – "New Identity"**

The creation of e-mail accounts only requires the data necessary for the e-mails (displayed name, e-mail address, server data etc.). Other data will not be queried.

---

### **Privacy – Rating**

- Privacy issues (law etc.) are documented: (partly +0.5)
- The user has freedom of choices concerning the identity management: (+1)
- The user is supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent: (+1)
- The IMA informs user about purpose of data processing or does not process personal data: (+1)
- The IMA informs completely about all used and transmitted personal data: (partly +1)
- Usage of pseudonyms / anonymity is possible: (+1)
- Usage of different pseudonyms is supported (+1)
- User is only asked for needed data overall: (+1)
- Only necessary data is processed (data minimisation): (+1)

### **Law Enforcement and Liability**

The Outlook Express 6 functions do not support Law enforcement nor Liability. Depending on the settings, the user and connection data are stored in the cache of the computer on which Outlook Express 6 is deployed. These data could be accessed by Law Enforcement Agencies.

Rating:

- Logging of transmitted e-mails / used account (+1)

### **Trustworthiness – Multilateral Security**

Multilateral security is not sufficiently supported. The identities are to be managed on the user's computer, and there is no known direct communication connection to the outside. The source code of Outlook Express cannot be viewed easily. The development is incumbent on the Microsoft company.

### **Trustworthiness – Seals**

Outlook Express has not been awarded with seals, yet.

### **Trustworthiness – Rating**

- The IMA provider / publisher is an established company being well observed: (+1)
- The IMA is fully under control of the user: (+2)

## **4.2.6.11 Platform and Environment**

### **Hardware, Software, Services**

The usage of Outlook Express 6 requires a computer on which one of the following operating systems is installed: Windows98, Windows 98 Second Edition, Windows Millennium Edition, Windows NT 4.0, Windows 2000, Windows XP 64-Bit Edition or Windows XP. The delivery of Windows XP already includes Outlook Express 6, the other operating systems include only older versions. For older versions of Windows XP, the installation of the Service Packs 1 is required additionally.

### **Installation, Maintenance, Use**

The installation of Outlook Express is generally carried out along with a current Windows operating system and does not require any extra set-up. Furthermore, it is freely available via

the internet pages of Microsoft<sup>182</sup> and can be installed via the internet by use of the appropriate installation buttons.

### **Technical Resource Requirements**

Outlook Express can be used by a single person. There will be no further costs for the deployment.

### **Availability**

Outlook Express is distributed.

### **Installation Base IMS**

Since Outlook Express is installed along with Windows operating systems by default, the user numbers are to be estimated very high. Specific numbers, also regarding the wide-spread pirate copies, are unknown.

### **Interoperability / Standards**

The usual transmission standards for e-mails (IMAP, POP3, HTTP) and formats (HTML, ActiveX, JavaScript, Java, MIME etc.) are supported. The identity management function is a non-standardised creation by Microsoft.

### **Guarantee for Trustworthiness**

The manufacturer is the US American Microsoft Corporation which delivers Outlook Express as a part of its Windows operating systems. It is well known that numerous products by Microsoft (e.g., Office2000, Windows XP etc.) try to establish internet connections when started, without the exact content of the transmitted being obvious. It is not known, however, that Outlook Express transmits internal data to Microsoft during on-line connections.

### **Legal and Contractual Framework / Nature of Provider**

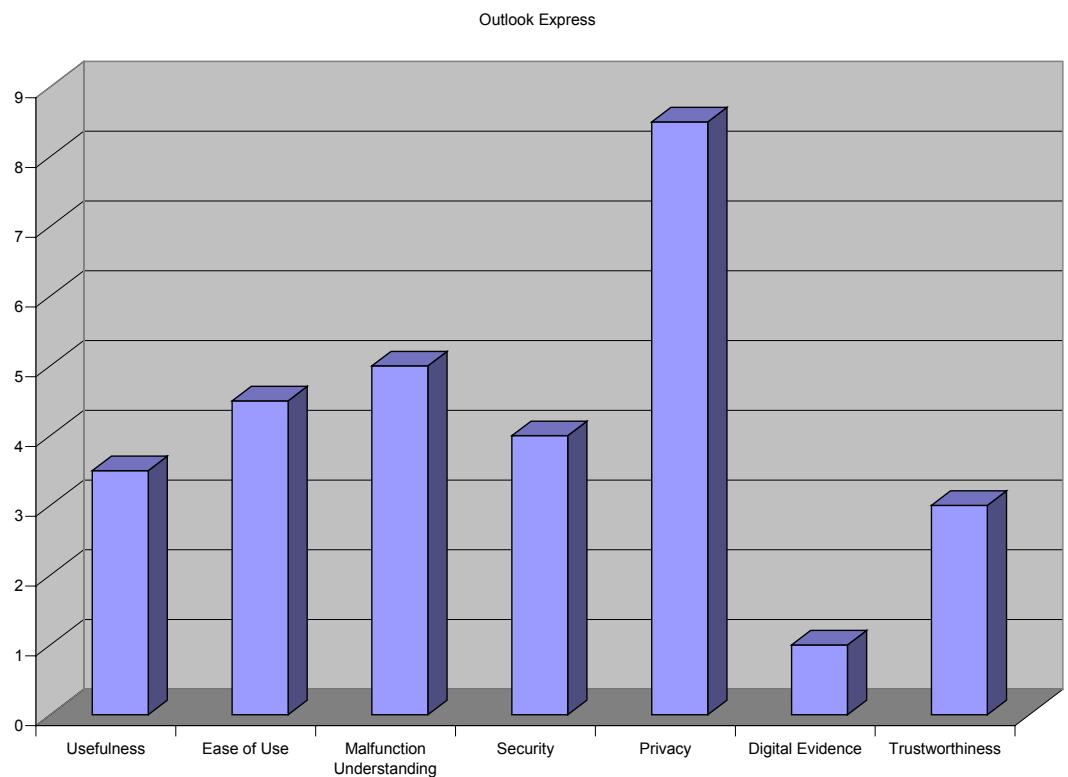
Microsoft is a world-wide operating group with its basis in the USA. There are branches in numerous countries, e.g., in most European countries.

#### **4.2.6.12 Conclusion**

The following chart shows the main evaluation results of Outlook Express normalised to 5 points maximum:

---

<sup>182</sup> <http://www.microsoft.com>.



**Figure 65: Overview Evaluation Outlook Express**

## 4.2.7 CookieCooker

When a user visits a web site and this web site sends a cookie to the user's computer, this cookie can be managed by the CookieCooker. On the one hand, this means that the user can view and delete the cookie. On the other hand, the user can exchange the cookie with other users to prevent a profile creation which is too exact.

Further on, CookieCooker is to recognise if a visited page requires the filling-in of a form. Here, the user can enter random data or completely or partly correct data. CookieCooker provides the opportunity to store these data and recall it at the next visit of this page. This applies to login data, too, whereby multiple data records can be stored and recalled alternatively.



Figure 66: CookieCooker – Main Window

### 4.2.7.1 IMS Category: Operational Area, Purposes and Functions/Interfaces

CookieCooker's functionality is to manage an arbitrary number of identities. Its features about cookies and identities are: usage of different identities at one web server, random choice of the identity to use, restriction of cookie storage to one session, exchange of cookies between users and assistance for the registration with a web service.

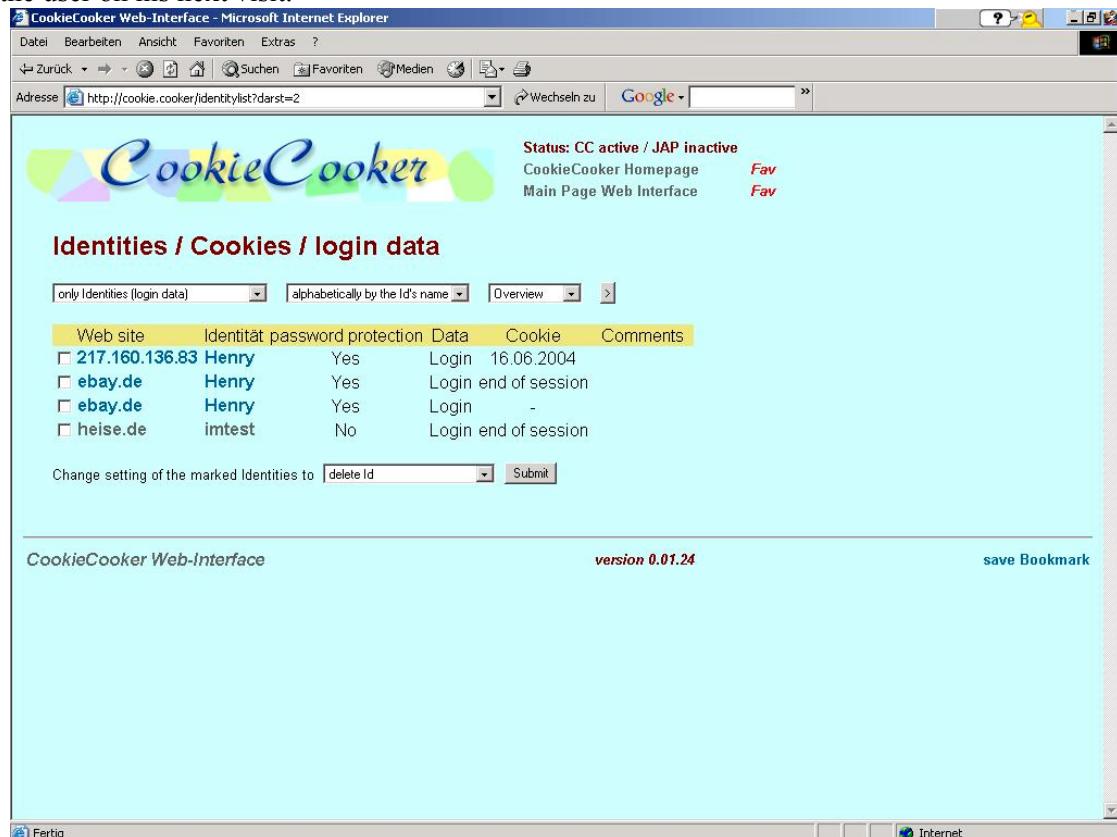
Figure 67: CookieCooker – Web Interface

---

The CookieCooker supports the anonymity application JAP, a software development within the Project "AN.ON – Anonymity.Online" sponsored by the German Research Foundation and the Federal Ministry of Economics and Technology<sup>183</sup>. Upon the user's wish, it will be embedded in the CookieCooker and can be controlled from there.

#### 4.2.7.2 Representation of Identities

CookieCooker can manage several identities for single web pages. In this context, both cookies containing corresponding data and direct entries in web forms are managed. The data entered in web forms (including the password) and the cookies that are possibly attached to that event are saved together as an "Identity". This is the set of data that the web server may use to recognise the user on his next visit.



The screenshot shows a Microsoft Internet Explorer window displaying the CookieCooker Web-Interface. The title bar reads "CookieCooker Web-Interface - Microsoft Internet Explorer". The address bar shows "http://cookie.cooker/identitylist?darst=2". The main content area has a light blue background with the "CookieCooker" logo at the top left. At the top right, there are links for "CookieCooker Homepage" and "Main Page Web Interface", each with a red "Fav" button. Below this, the heading "Identities / Cookies / login data" is displayed. A table follows, with columns: "Web site", "Identität", "password protection", "Data", "Cookie", and "Comments". The data in the table is as follows:

Web site	Identität	password protection	Data	Cookie	Comments
217.160.136.83	Henry	Yes	Login	16.06.2004	
ebay.de	Henry	Yes	Login	end of session	
ebay.de	Henry	Yes	Login	-	
heise.de	imtest	No	Login	end of session	

Below the table, there is a dropdown menu "Change setting of the marked Identities to" with options "delete Id" and "Submit". At the bottom of the interface, there are links for "CookieCooker Web-Interface", "version 0.01.24", and "save Bookmark". The status bar at the bottom of the browser window shows "Fertig" and "Internet".

Figure 68: CookieCooker – Web Interface: "Identities..."

The identities can be real names, but also pseudonyms.

#### 4.2.7.3 Handling of Identities

CookieCooker also supports the user in the creation and input of pseudonyms by suggesting random data. The user can select the appropriate pseudonym at a later visit of the page. The data can be viewed, modified, or the pseudonym or cookie can be deleted at any time.

#### 4.2.7.4 History Management

CookieCooker gives the user an overview of his identities and records their usage. Thereby he can see where, when and how which data was sent to a server.

---

<sup>183</sup> [http://anon.inf.tu-dresden.de/index\\_en.html](http://anon.inf.tu-dresden.de/index_en.html).



Figure 69: CookieCooker – Cookies and Identities

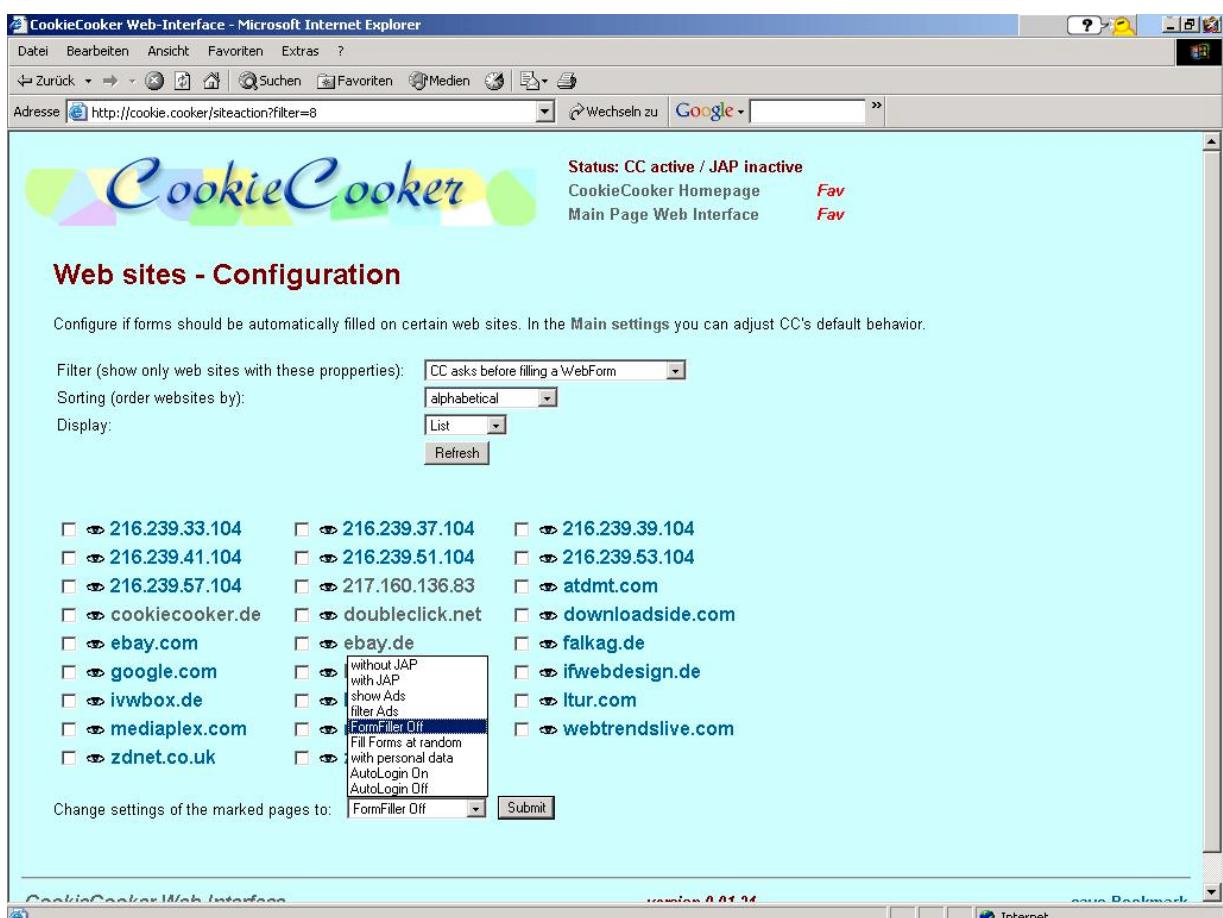
#### 4.2.7.5 Context Detection

CookieCooker can detect a part of the form queries by web sites and make appropriate suggestions for the entries. It is then possible to use the data preconfigured by the user, or CookieCooker selects random entries from a database with didactically correct entries such as street names that make sense. Form queries that are unknown to the program will be left undone.

#### 4.2.7.6 Rule Handling

For single web pages, the following individual settings can be defined:

- Without JAP
- With JAP
- Show Ads
- Filter Ads
- FormFiller Off
- Fill Forms at random
- Fill Forms with personal data
- Autologin On
- Autologin Off



**Figure 70: CookieCooker – Configuration**

#### 4.2.7.7 Privacy Control Functionality

The users are not specifically supported in asserting their privacy rights such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent.

CookieCooker provides the opportunity to enter random data that look like authentic data to the web server that evaluates the form in forms. This prevents the user from entering personal data.

The exchange of cookies via various Exchange Servers is to prevent operators of web pages from being able to create profiles of their visitors. Those who evaluate a cookie cannot be sure that those who stored a cookie on the hard disk is actually the one who triggered the cookie. If this function is deployed extensively by numerous users, a profile maintenance would become impossible.

CookieCooker does not exchange all cookies, though, in order to prevent the passing-on of personal data. CookieCooker uses several ways to find out if personal information is connected to a cookie for preventing the cookie to be exchanged. If only one of the signs indicates a connection to personal information, CookieCooker marks that cookie as not exchangeable. Signs are e.g.: Personal data has been entered in a form, username or password have been sent, the site is set to "green" (trustworthy).

#### 4.2.7.8 Identity Recovery

CookieCooker provides an Identity Recovery function. Deleted identities are at first moved to the trash can. The trash can keeps deleted identities until the user exits the CookieCooker. After exiting CC the trash can will be purged and no further identity recovery is possible.

#### 4.2.7.9 Digital Evidence Functionality

CookieCooker has no digital evidence functionality.

#### 4.2.7.10 Categories

##### Usability – Perceived Usefulness

The form fill-in function accelerates the filling-in of web forms. Random data that make sense can be suggested without the user having to invent such data on his own. Alternatively, the CookieCooker can insert data which have been predefined by the user. Furthermore, CookieCooker simplifies the management of access data. The CookieCooker notices when the user enters access data and stores them along with the corresponding cookie within an identity. At a later visit of the page, the CookieCooker enters the access data automatically, i.e., it is not necessary to write down the data anywhere else or keep them in mind.

Rating:

- Application benefits usage several times a month: (+1)
- Application benefits every day usage: (+1)
- Time for first time adjustment is less than time for action without IMA: (partly +0.5)
- After first time adjustment the action is faster as without IMA: (+1)
- After first time adjustment the action is more than twice as fast as without: (+1)

##### Usability – Perceived Ease of Use

At first, the variety of functions is quite irritating. After the correct installation, different pop-up windows appear in various situations. These pop-up windows require reactions from the user without providing more detailed information on the offered options, though. However, most of the functions are self-explaining. Not every pop-up window provides the opportunity to cancel in order to put a decision aside, though. Also the "X" button in the top right window corner does not always work, e.g., in the "Select identity" window.

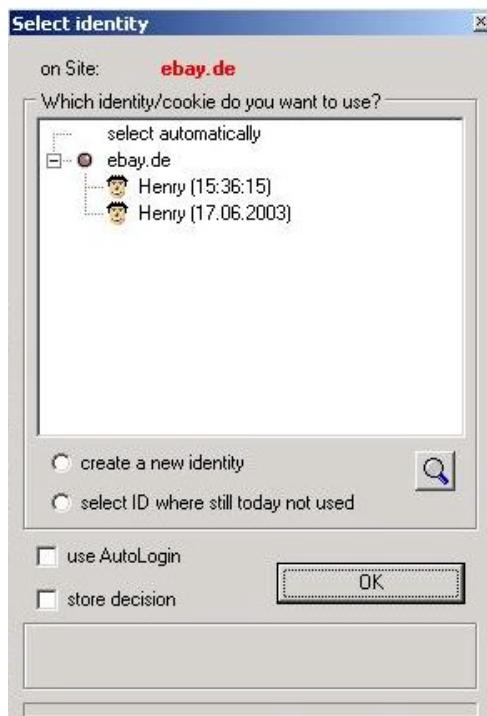


Figure 71: CookieCooker – "Select Identity!"

---

A detailed manual or help file is not provided. Many functions can only be understood after a few try-outs. Only a short description of the basic functions can be found on the main page of the CookieCooker<sup>184</sup> and in a FAQ.

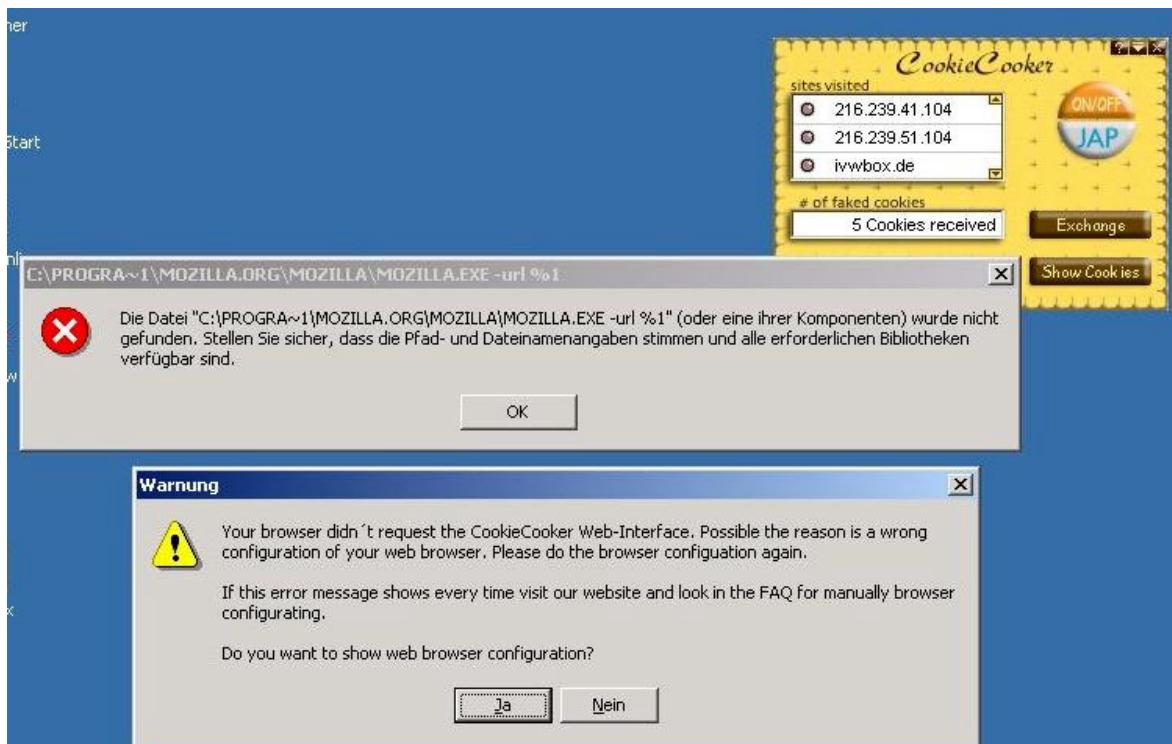
The CookieCooker provides the opportunity to modify its settings both directly within the main application and via a web interface which can be activated with a double click on the CookieCooker icon in the menu bar or by the appropriate selection in the main application. These different adjustment interfaces can irritate and unnerve the user.

Rating:

- After a period of vocational adjustment the user is able to use the function autonomously: (+1)
- It is not necessary to consult external support: (+0.5)
- No previous knowledge is needed: (+0.5)

### **Usability – Malfunction Understanding**

On the test system, the CookieCooker web interface could not be started at first.



**Figure 72: CookieCooker – Malfunction Understanding**

The reason for that behaviour was the configuration of the Internet Explorer for the CookieCooker while Mozilla 1.4 was the preset standard browser. The CookieCooker reported: "Your browser didn't request the CookieCooker web interface. Possible the reason is a wrong configuration of your web browser. Please do the browser configuration again." A new configuration did not fix the error, though. Only after extensive research and some try-outs revealed the solution concerning the change of the standard browser.

Rating:

- The user can recognise that an error occurred: (+1)
- In case of a malfunction the function presents a complete and understandable description of the error: (partly +1)
- There are suggestions for what to do next: (+1)

---

<sup>184</sup> <http://www.cookiecooker.de>.

### **Security – Confidentiality**

To protect the personal data of the user CookieCooker offers the possibility to encrypt all data that is stored on the hard disk. The data is encrypted with the symmetric Rijndael algorithm. The password that the user enters will be used as a key for the encryption.

Although the CookieCooker evaluates single cookies according to the data they contain (personal or not) it cannot fully be excluded that cookies with valuable data are passed on. An assignment to a particular person would be quite difficult then but cannot be excluded, too, regarding the content of the cookie. Although the CookieCooker provides the opportunity to view the cookies prior to the exchange and prevent the exchange, if applicable, but due to the masses of appearing cookies, hardly any user would do this.

Another security risk is represented by the display of identities. The stored access data or form entries are displayed in plain text and can therefore be viewed by everyone who can see or operate the screen. In this context, the function "password list" which lists all stored passwords in plain text is particularly dangerous. The usage of the CookieCooker can be linked with a password entry but the default settings do not require this.

### **Security – Integrity**

The storage of the data managed by the CookieCooker can be carried out in encrypted form if the user activates this option.

### **Security – Availability**

During the test period in June and July 2003, there were no system downtimes.

### **Security – Rating**

- The stored data is encrypted: (optional: +1)
- Transmitted data is encrypted: (optional: +1)
- Data access and manipulation is only possible after authentication: (optional: +1)
- Backup & restore of data is (manually) possible with adequate effort: (+1)
- IMA informs completely about all processed and transmitted personal data: (+1)

### **Privacy – User Empowerment**

CookieCooker provides the user with the opportunity to define which cookies are to be distributed. The user can also define which data are to be transmitted via the form fill-in function and which data are to be stored.

### **Privacy – Transparency**

The CookieCooker cannot manage old, already present cookies. In order to make sure that the CookieCooker controls all cookies, the user is offered the option to remove the old cookies during the installation process. This refers only to the cookies used by the deployed browser, though. If another browser is in parallel use (during the test, we used the Mozilla 1.4), its cookies are not affected. The CookieCooker does not notify the user about this.



**Figure 73: CookieCooker – "Delete old Cookies"**

The cookie exchange is carried out via Exchange server. Due to the used principle, there is the risk that the operators of the Exchange servers store these cookies containing the profile data along with the user's IP in order to create profiles again.

A Privacy Policy could not be found on the CookieCookers web site. P3P is not supported.

#### **Privacy – Data Minimisation**

Data minimisation – reduction of processed personal data; use of pseudonyms / anonymity; unlinkability – is not in the focus of this IMA.. CookieCooker does not require any personal information for its usage. However, for the Form Fill-In function, personal data can be entered (but do not have to since they are not definitely necessary for this function).

According to the determination of the CookieCooker, numerous pieces of information will be collected with the deployment of the access data management, which are stored on the user client, though, and are not transmitted without the user's permission.

#### **Privacy – Rating**

- Privacy issues (law etc.) are documented: (+1)
- The user has freedom of choices concerning the identity management: (+1)
- The user is supported by privacy control functionality such as information about personal data stored at a server, allowing access to these data, give the means to correct these data, to remove them, or to grant or revoke consent: (+1)
- The IMA informs user about purpose of data processing: (+1)
- The IMA informs completely about all used and transmitted personal data: (yes, but difficult to understand +1)
- The IMA adheres to EU privacy standard: (+1)
- Usage of pseudonyms / anonymity is possible: (+1)
- Usage of different pseudonyms is supported (+1)
- User is only asked for needed data overall: (+1)
- Unlinkability / anonymity of data is supported: (+1)

### **Law Enforcement and Liability**

The functions of CookieCooker do not support law enforcement or liability. On the Exchange servers, there will be – at least temporary – connection data which could be accessed by Law Enforcement Agencies in connection with the transmitted cookies.

Rating:

- Log function about used pseudonyms (+1)

### **Trustworthiness – Multilateral Security**

Multilateral security is not sufficiently supported. The CookieCooker has originally been developed at the Technical University of Dresden. The current Version, however, is only available for a certain registration fee.

The current source code of the CookieCooker cannot simply be viewed.

### **Trustworthiness – Seals**

There are no seals for the CookieCooker.

### **Trustworthiness – Rating**

- The IMA is fully under control of the user: (+2)

#### **4.2.7.11 Platform and Environment**

##### **Hardware, Software, Services**

CookieCooker available for Windows operating systems (Windows 98, ME, 2000, XP) only. Windows 95 is not supported, though. CookieCooker can be installed on all computers on which these systems are operated.

The price for the CookieCooker is 15,- Euro for registration. The registration fee can be paid by credit card or bank transfer. The user gets two registration keys (the second as a coupon). With those he/she can install CookieCooker with two different Windows user names or on two different computers. After installing CookieCooker it will work for 7 days without any restrictions and free of charge.

##### **Installation, Maintenance, Use**

After the CookieCooker has been downloaded from the Internet or received from somewhere else, only the appropriate file has to be executed. In order to be able to work, the CookieCooker requires that the deployed browser is configured for the usage of the CookieCooker. CookieCooker offers to carry out the configuration automatically and displays the detected browsers for selection. On the test system, both the Internet Explorer 6 and the Mozilla 1.4 were installed. CookieCooker detected the first one only, though.

Furthermore, the CookieCooker offers to configure the system to allow the usage of the anonymising tool "JAP", too.



**Figure 74: CookieCooker – JAP Integration**

Then the installation allows the user to set that the CookieCooker should run every time when the users is surfing in the internet.

During the test, there were problems with the proxy configuration. Previous to the installation of the CookieCooker, the test system was configured in a way that the connection to the internet was diverted via a proxy. This had not been detected by the CookieCooker, i.e., a manual configuration was necessary. The required data could only be identified after an extensive search on the web site of the provider.

If a standard system is deployed during the installation, the installation will only take a few minutes. In special cases, more time might be necessary due to the missing documentation.

### **Technical Resource Requirements**

A CookieCooker licence is available for 15 Euro. The registration fee can be paid by credit card or bank transfer. But the user can test the software. This means that after installing CookieCooker it will work for 7 days without restrictions and free of charge. After registration the user gets two registration keys. With those he can install CookieCooker with two different Windows user names or on two different computers.

### **Availability**

The CookieCooker is distributed by the site [www.cookiecooker.de](http://www.cookiecooker.de).

### **Installation Base IMS**

The number of installations is not known. Since earlier versions of the CookieCooker have been distributed freely, the number of registrations cannot be the basis for consideration. According to statements by the programmers of the CookieCookers, there are about 1,500 to 2,500 permanent users. The number of free downloads is estimated at 20,000.

### **Interoperability / Standards**

The CookieCooker can be used in connection with the anonymising software JAP<sup>185</sup>.

<sup>185</sup> [http://anon.inf.tu-dresden.de/index\\_en.html](http://anon.inf.tu-dresden.de/index_en.html).

### Guarantee for Trustworthiness

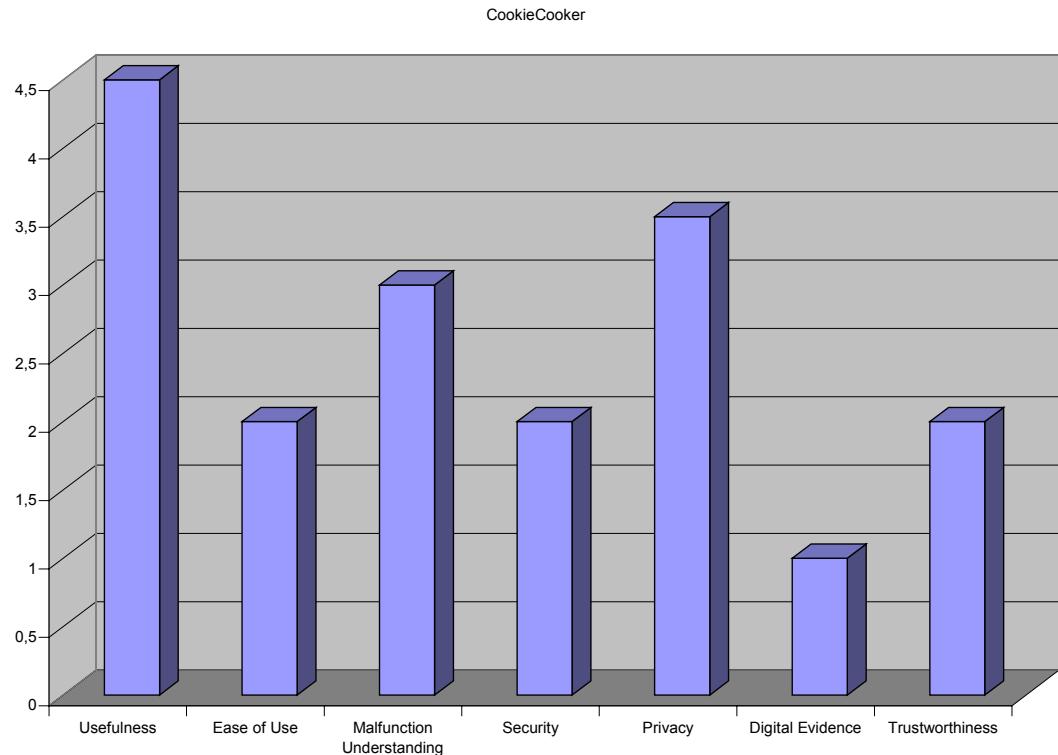
CookieCooker is not an Open Source Project. It is distributed by a private association. There are no external guarantees of trustworthiness.

### Legal and Contractual Framework / Nature of Provider

The CookieCooker is developed at the German Technical University of Dresden and is now distributed by a private association.

#### **4.2.7.12 Conclusion**

The following chart shows the main evaluation results of CookieCooker normalised on 5 points maximum:



**Figure 75: Overview Evaluation of CookieCooker**

## 4.2.8 Other Interesting Approaches

The following approaches of Identity Management Applications will be only shortly outlined. Partly they are research projects like ATUS or DRIM and situated under research and development. Other producers like Sun keep in mind basically the organisations and less the identity management of the single user. At last there are appendages like Digital Identity which are based on well-known technologies to give the user the facility to manage parts of his identity himself.

### 4.2.8.1 Freiburg iManager / ATUS

The Freiburg iManager is a module of "ATUS – A Toolkit for Usable Security", being developed at Freiburg University in a publicly funded project. In contrast to other IMA, the developers of the iManager not only regard identity configuration and identity negotiation as important functions, but also an accountability component which is responsible for integrating digital signature mechanisms. The developers stress that identity management has to integrate anonymity functionality. The iManager fulfils this requirement by offering an interface to an anonymity service.

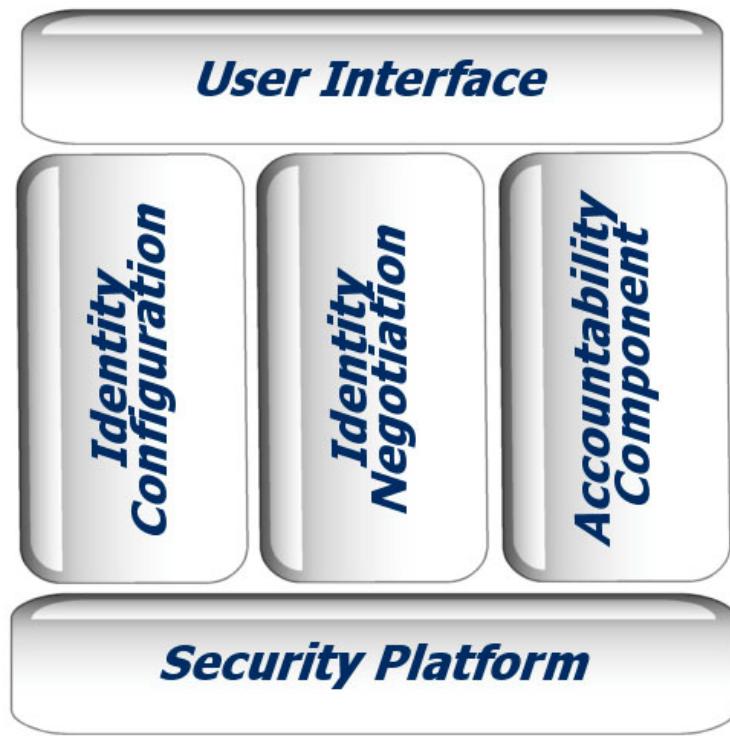


Figure 76: ATUS – Components

Figure 76 describes the components of ATUS. The architecture is shown in Figure 77 where components like context sensing, choice of identity and configuration of services perform the central work of identity management [Jendricke/Kreutzer/Zugenmaier 2002]. An additional situation database is proposed for later implementations. The iManager and ATUS only work on a unilateral basis, i.e., the user is acting on his own protecting himself, not having to rely on other parties. The software, realised as a proxy for use with a standard browser, allows certain functionality [Jendricke/Gerd tom Markotten 2000], always considering usability aspects, e.g., by offering predefined role-modes such as shopping or anonymous surfing.

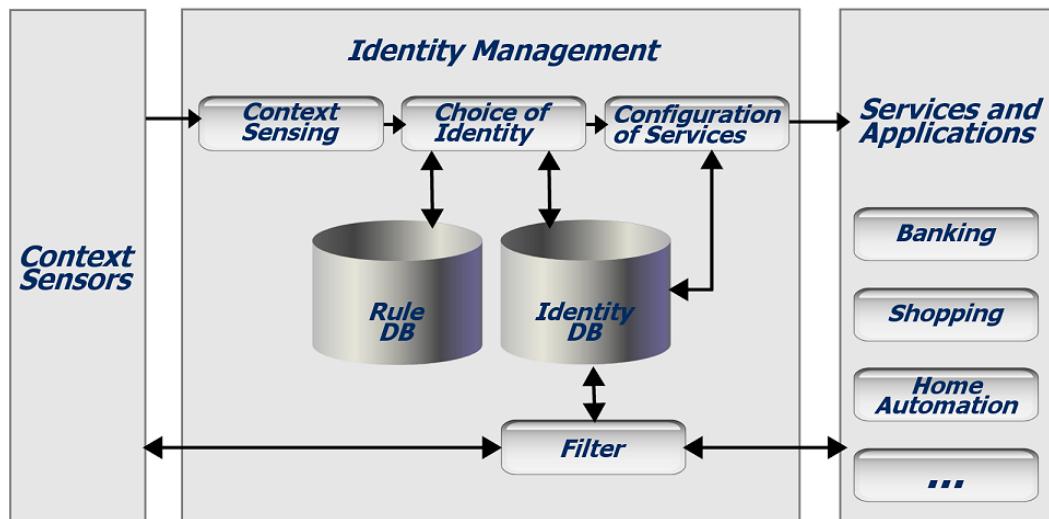


Figure 77: ATUS – Architecture

The iManager is realised as a prototype for an Internet browser and for a PDA.



Figure 78: ATUS – Snapshot PDA Version

#### 4.2.8.2 DRIM

DRIM – Dresden Identity Management<sup>186</sup> is a university project which has the vision to implement a comprehensive IMS.

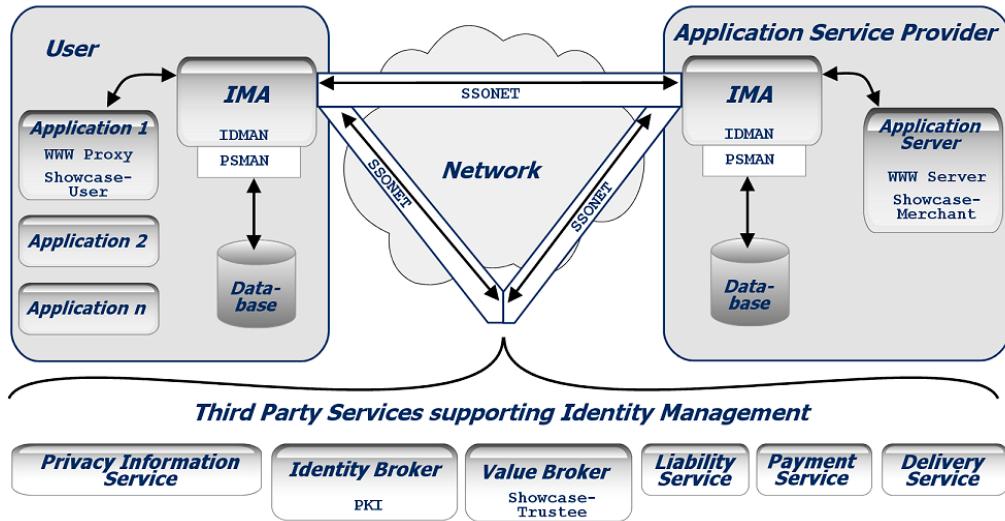


Figure 79: DRIM – Architecture and Available Components

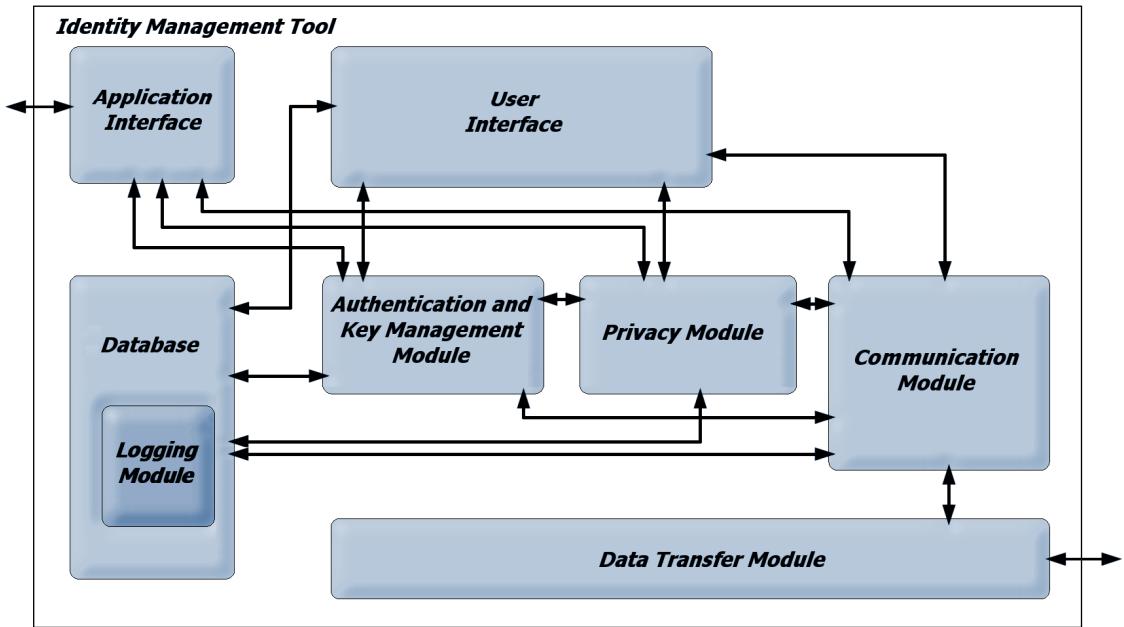
DRIM is being developed at Dresden University of Technology strictly following the principles of multilateral security, taking into account the manifold of possible co-operating parties. Thus, a really privacy-enhancing IMS could be achieved. Figure 79 depicts the architecture design and the components already available (shown in typewriter font).

Among others, a strong anonymising service (AN.ON), a security toolkit (SSONET: Security and Privacy in Open Networks [Pfitzmann/Schill/Westfeld et al. 1998])<sup>187</sup> and a credential mechanism (idemix<sup>188</sup> from IBM) are integrated in the development.

<sup>186</sup> <http://dud.inf.tu-dresden.de/~kriegel/DrimWeb/>.

<sup>187</sup> [http://wwwrn.inf.tu-dresden.de/RESEARCH/ssonet/ssonet\\_eng.html](http://wwwrn.inf.tu-dresden.de/RESEARCH/ssonet/ssonet_eng.html).

<sup>188</sup> <http://www.zurich.ibm.com/security/idemix/>.



**Figure 80: DRIM – Internal Structure of the Client**

The user's IMA is the main component of the system. It acts as a central gateway for all communication of different applications, like browsing the web, buying in Internet shops or performing administrative tasks at governmental authorities. The IMA will have the following functionality (cf. Figure 80):

- A privacy module, which negotiates with the communication partner about dissemination of (personal) data and pseudonym types to use;
- A pseudonym and key management module, which creates and manages pseudonyms, cryptographic keys and certificates associated with the pseudonyms and which communicates with key servers;
- A logging module, which logs context information about ongoing transactions, e.g., communication partners and exchanged (personal) data;
- A database, which holds all the data needed at the user's side, i.e., pseudonyms, cryptographic keys, certificates, elements of (personal) data, information about communication partners and context information about ongoing and finished transactions;
- A secure communication module, which enables encryption, integrity, (pseudonymous) authentication, as well as usage of anonymity services;
- A user-friendly GUI, which consists of different levels of detail for management and configuration of pseudonyms, digital identities, cryptographic keys and certificates, and for viewing and evaluating logging information.

These modules cover the main requirements for the user side of an IMS. All these modules must be under the control of the user, but not necessarily in one location or integrated in one device – likewise a distributed realisation is possible. E.g., the GUI can be implemented on (less capable) mobile devices while the other modules are located at a more powerful fixed station, using secure communication to the external GUI. The IMS should support both being operated by the user and by a trusted provider – the user should get the opportunity to decide which setting is appropriate for his requirements.

The IMA tools at the application services are needed primarily to handle anonymous or pseudonymous requests, and especially pseudonymous authentication of users. So the following functionality is needed:

- Managing policies for accepting or denying user requests;
- Negotiating about requesting (personal information) from the user;
- Checking certificates submitted by the user;
- Providing information about necessary linkability or pseudonym properties.

The various third party services are needed to enable users to use application services in a privacy-preserving way, e.g., by an additional separation of knowledge.

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

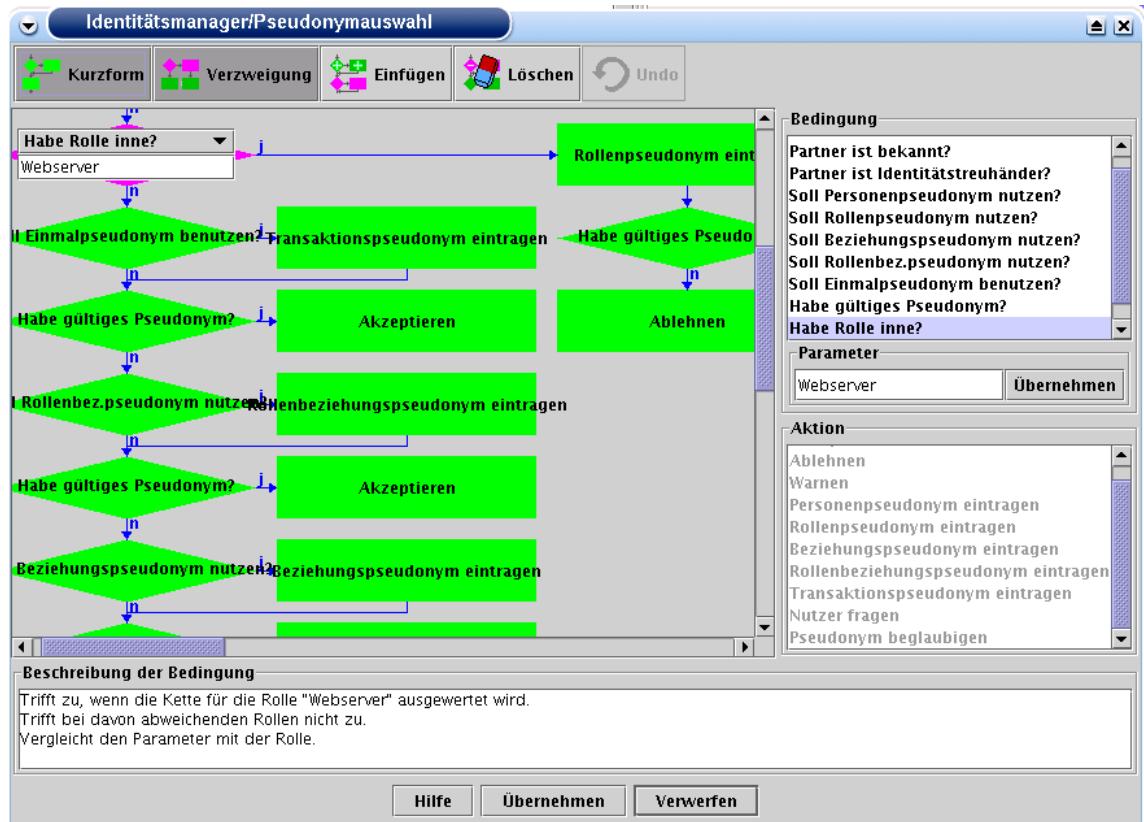


Figure 81: DRIM – Creation of Pseudonyms

**4.2.8.3 Sun One**

The identity management of Sun One is based on four services:

1. Directory Service: user profile data (public keys, certificates, access authorisation) are stored and managed. This is based on a central repository.
2. Access Management Service: Administration of access authorisation. Based on role-based Policy Management
3. Provisioning Service: Regulation of the access to services and resources by users / the system
4. Identity Administration Services: Management and Administration of identities

For these services, Sun offers two hardware components:

1. Sun One Portal Server: a Server which is to enable a secure user and community Management, the personalisation of web information, the aggregation and integration of user data and a quick search for these data.
2. Sun Directory Server 5.1: Central repository for the storage and management of user profiles, access authorisation and information on application and network resources.

---

#### **4.2.8.4      Digital Identity**

Digital Identity is a product by Ascio Technologies Inc<sup>189</sup>. Their headquarters is residing in Copenhagen, Denmark. Another office is located in Munich, Germany. Ascio is a provider of domain registration technology to domain resellers, Telcos, and ISPs. Ascio has created a unique distributed hosting technology, using the Domain Name Service (DNS), which provides a location for personal information in a number of security layers that allows for varying degrees of access. At the basic level the user can maintain a secure on-line database for all personal information including personal organisation tools such as a calendar and address book. The aims of Digital Identity are:

- to provide one universal Internet address
- to further enable e-commerce through the provision of one universal account
- to provide consumers with one on-line repository for information and resources.

Digital Identity provides end users with an opportunity to take ownership of their presence on the internet through the provision of a universal address that is accessible from any computer that is Internet compatible. It enables users not only to personalise information, but also set access levels for friends, family or businesses. As said on the internet side of Digital Identity<sup>190</sup>: each individual is assigned a personal web address that functions as a master key to all his or her on-line communication: on-line business cards, CV, 'My Pages', favourites, personal messages, access control etc. The individual creates and has full control of their on-line information. With Digital Identity each individual becomes an integrated part of the Internet, so other web sites, search engines and applications automatically can interact with the on-line identity.

---

<sup>189</sup> <http://www.ascio.com>.

<sup>190</sup> <http://www.digital-identity.info>.

#### 4.2.8.5 Open Privacy

"OpenPrivacy.org is building an Internet platform to take us into the next age – the age of secure personalised information. Basic to this goal is a platform that will provide people with complete control over their personal information and aid them in protecting their privacy while simultaneously enabling more efficient data mining by marketers and the access to highly desirable market segments by advertisers.

OpenPrivacy creates a secure marketplace for anonymous demographic and profile information, and a distributed, attack-resistant, reputation-based rating system that can be used for everything from item selection and ordering to search result filtering. Further, this system is completely open, allowing multiple communication mechanisms, languages and ontological meanings to coexist. This platform thrives on diversity.

To accomplish our goals, we introduce three new concepts: Opinions, Bias and Reputations. These are all first class, signed objects that are created at will under a multitude of pseudonymous entities maintained by the user. A fourth concept, that of a personal profile, is created virtually from a collection of the first three objects in such a way that only the owner of the information can validate the connections between them. However, if granted access, others (marketers, advertisers, on-line community builders and the like) may mine the profile for potentially profitable or otherwise valuable correlations while the owner of the profile maintains her anonymity."<sup>191</sup>

The newest information on the web site of OpenPrivacy are from summer 2001<sup>192</sup>. It seems that this project is not enhanced anymore.

---

<sup>191</sup> <http://www.openprivacy.org/papers/200103-white.html>.

<sup>192</sup> <http://www.openprivacy.org/news.shtml>.

---

#### **4.2.8.6 IBM WS-Security**

"WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

WS-Security also provides a general-purpose mechanism for associating security tokens with messages. No specific type of security token is required by WS-Security. It is designed to be extensible (e.g., support multiple security token formats). For example, a client might provide proof of identity and proof that they have a particular business certification.

Additionally, WS-Security describes how to encode binary security tokens. Specifically, the specification describes how to encode X.509 certificates and Kerberos tickets as well as how to include opaque encrypted keys. It also includes extensibility mechanisms that can be used to further describe the characteristics of the credentials that are included with a message."

#### 4.2.8.7 American Express Private Payments

Private Payments is a free on-line service for American Express Card-Members that should make shopping on the internet more secure. Private Payments numbers can be used at any website that accepts the American Express Card. Private Payments enables American Express Card-Members to use an instantly generated, limited-life, transaction number instead of a card-member's actual Card number to make purchases on-line. American Express is able to match this transaction number to the registered American Express Card of the user, so that all Private Payments purchases are recorded and billed directly to the actual American Express Card account. As a result, the monthly American Express Card statement will include all transactions the user has made during the billing period, whether they were made using a Private Payments number or the actual American Express Card account number<sup>193</sup>.

---

<sup>193</sup> <http://www26.americanexpress.com/privatepayments/faq.jsp>.

## 4.2.9 Summary

Table 30: Comparison of Identity Management Applications

Application	Main Functionality	Type of ID	Usefulness	Ease of Use	Malfunction Understanding	Security	Privacy	Digital Evidence	Trustworthiness	Cost for User	Business Model
Microsoft Passport	SSO	centralised	4	4	2	4	4.5	0	1	0	Paid by partner sites
Liberty Alliance	SSO	federated	4	2+X	X	4.5+X	3.5+X	0	2+X	0	Paid by partner sites
Yodlee	SSO	centralised	4	3.5	4	10	5	0	1	0	Presentation / Promotion
Mozilla Navigator	Form Filler	federated (client)	4	4.5	4	6	9	0	3	0	Open Source
Digitalme	Form Filler	centralised	4	3.5	2	7	9	1	1	0	Presentation / Promotion
CookieCooker	Form Filler	federated (client)	4.5	2	3	5	10	1	2	15 €	Paid by user
Outlook Express	Mail Identities	federated (client)	3.5	4.5	5	4	8.5	1	3	0	Part of MS Windows

None of the analysed applications and systems is without weaknesses (cf. Table 30). Some belong to general problems of the main functionality, some are home-made.

The both global big systems with single sign-in functionality, Microsoft Passport and Liberty Alliance, have their own weaknesses. The actual version of Microsoft Passport has in particular deficiencies in security, privacy, interoperability, and malfunction understanding. Regarding Liberty Alliance the evaluation of some parts which are dependent on the implementation could not be performed.

Form filling functionality is a low-end kind of identity management. Mozilla Navigator, Digitalme and CookieCooker present this functionality but have shortcomings in usability, security and privacy. The password management functionalities of Digitalme and Mozilla Navigator base on comparable functions and have comparable deficiencies.

The handling of identities is solved most suitable of Novel Digitalme but is usable with all applications. A greater extend of the representation of identities and adoption of different kinds of identities you can find at Mozilla Navigator, Liberty Alliance and Digitalme. But primary new projects like DRIM of the TU-Dresden will propagate particularly the usage of different kinds of pseudonyms.

Identity recovery functionality is only implemented partly in the CookieCooker. The users of all other tested applications have no chance to retrieve by mistake deleted data. Similar is the availability of history management.

Only Liberty Alliance, Microsoft Passport and CookieCooker have nameable functionality of rule handling and context detection. But they approximate this functionality just partly.

Privacy is attended by all tested applications in different specificity. Microsoft Passport has agreed to extend his privacy functionality. Only CookieCooker has a bigger orientation to the privacy aspect.

It's a main result of this Chapter that all tested Identity Management Applications show weaknesses. The target directions of the functions vary from each other in a way that makes a comparison quite difficult.

Some of the weaknesses are caused by the concepts and are based on the product philosophies of the individual providers. An important customer decision when selecting the products would thus be the question if the data management and maintenance is to be carried out by an outside company or on the own systems. Products such as Microsoft Passport, Novell Digitalme or Yodlee require the user's trust in the IMS Provider to whom the data is given. In this context, Liberty Alliance provides the opportunity to distribute the data maintenance among several

providers and keep a higher level of control of its usage in one's own hands. However, this solution does not work without confidence in the companies connected to a Circle of Trust.

As far as privacy protection is concerned, the IMA that maintain the data directly on the user's systems, like e.g., Mozilla, CookieCooker, Explorer and new inventions such as DRIM or ATUS would be to be preferred. However, even with this solution, the manufacturers must be trusted that they have not included any backdoors which allow espionage. This confidence would generally be on a higher level with Open Source products like Mozilla than with products by market-ruling companies like Microsoft. Standards like P3P for the improvement of transparency concerning Privacy Protection are hardly considered.

Liability is not supported actively by the tested products. If legally important actions are carried out, the perpetuation of evidence is left to the user. With e-mail clients, this can take place, e.g., via the deployment of digital signatures, whereas the signed mails have to be maintained by the user. Even subsequent signing in cases of, e.g., a compromising of a signature technology has to be done by the user, or he has to switch to other products.

It cannot be foreseen to which extent digital evidence is stored for law enforcement purposes. Wherever central IMS providers are involved, the user's entire communication can generally be recorded. The documentation of the tested products do not provide any information on possible interfaces to criminal prosecution authorities or backdoors.

History functions are provided – if provided at all – in an only rudimentary manner. Although an automatic third party logging may be unwanted for privacy protection reasons, the user should at least be provided with the opportunity to recall carried-out actions. For example, Novell Digitalme provides the opportunity to view who has gained access to meCards. History functions can also help to detect and record hacking attempts.

The usability of many of the products, too, is insufficient. For example, many functions of the CookieCooker can only be understood after having been tried out or remain in the dark. Problems of Microsoft Passport with browsers like Mozilla are not mentioned explicitly, and the user is confronted with wrong error messages.

It is definitely the interaction of usability, security and privacy that needs developmental work on all products to convince the user that the deployment of IMA makes sense.



## 5 [CHAPTER E: DESIGN OF AN IDENTITY MANAGEMENT SYSTEM]

In this Chapter we describe the most relevant and common IMS models and architectures. The main differences are identified in certain concepts of data flow, data storage and the expected trust models. We point out advantages and disadvantages, strengths and weaknesses with respect to those different approaches.

### 5.1 Basic Architectures

We distinguish three basic IMS architectures with regard to the position of IMS in the data flow. This shall be highlighted in the following figures, where a user at the client-side (left) establishes a connection to some digital service or network, using an IMA and the appropriate application.



Figure 82: Basic Model: IMA ↔ Application ↔ Digital Services

The first model, shown in Figure 82, presents a normal communication between an application and a digital service where the user adds the IMA. This means that he directly communicates with the IMA, which contains all identity information. The output of the IMA can already be pseudonymised so that the application will use a pseudonymous data as input, probably not knowing the real identity. The application may be a web browser or a web service the IMA on the user's client connects to.



Figure 83: Basic Model: Application ↔ IMA ↔ Digital Services

In Figure 83 the order of the application and the IMA is reverted, so that the user communicates directly with the application, which uses an IMA while accessing a digital service. As the IMA in Figure 82, it stores personal information about the user. This approach is more universal than the one shown in Figure 82 as many applications can use this IMA as a gateway. The IMA can be realised as proxy. This basic model does not reveal information about the location of the IMA, which might be as well in the client area as in the server area of an IMS provider.

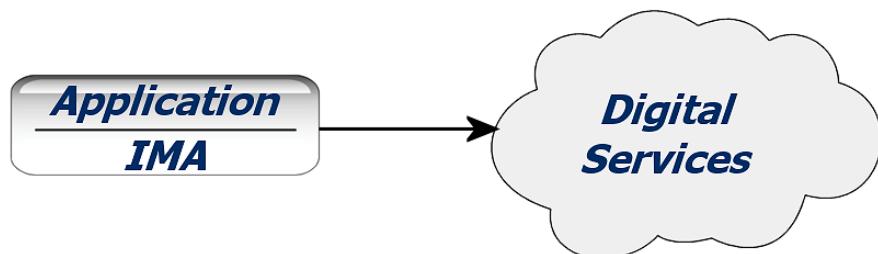


Figure 84: Basic Model: IMA in Application ↔ Digital Services

Figure 84 illustrates a combination of application and IMA, i.e., the IMA can be a component within the application, being realised at the same location. In contrast to Figure 83 it is not clear whether this IMA module consists of open interfaces so that other applications can make use of it, too. Thus, its use may be restricted to only one or few applications. An advantage might be that the IMA can be tailored specifically according to the needs of the application, e.g., the interpretation of context might be easier, and the information on desired pseudonym properties more specific, the support more user-tailored.

## 5.2 Different Zones of Trust

For user-controlled identity management – no matter which basic model applies – the data storage and processing has to happen in a zone, which the user trusts.<sup>194</sup> In this Chapter two different trust models [Gerck 1998; Grandison/Sloman 2000] are described:

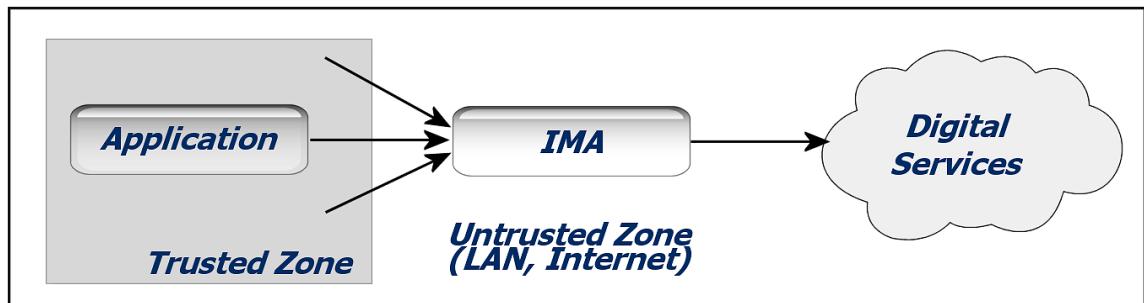


Figure 85: Limited Trusted Zone

In Figure 85 the trusted zone is quite small: The user only trusts the application area (presumably within his own device), whereas the IMA is located in a non-trusted zone (presumably outside his device, e.g., in the Internet). This means that storage and processing of (sensitive) identity data cannot (fully) be handled under user-control.

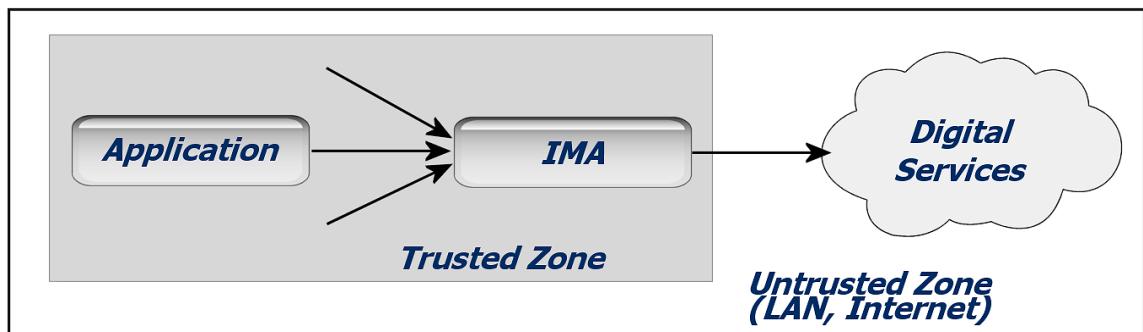


Figure 86: Enhanced Trusted Zone

Figure 86 extends the trusted zone so that it comprises the application and the IMA. Examples for this configuration are the Reachability Manager, i.e., a PDA<sup>195</sup> with an integrated identity management component [cf. Damker/Pordesch/Reichenbach 1999], or a Personal Computer that offers an IMA trusted by its user.

The IMA might be realised as a (trusted) proxy so that it can be interposed in digital communication. This proxy can be located on the user's computer, on a server, e.g., of one's access provider or of the employing company or on the server of an IMS provider. The location does not mean automatically that a system is being trusted or not trusted to a certain extent. So obviously a system at the user's side offering the possibility for directly controlling the device

<sup>194</sup> Of course user trust depends upon many factors [Egger/Abrazhevich 2001].

<sup>195</sup> Trustworthy user devices are analysed, e.g., in [Pfizmann/Pfitzmann/Schunter/Waidner 1999].

might be considered to be more trustworthy. Commonly, users will trust their telecommunication providers or financial institutes to a larger degree than only to their core business. In this end, the amount of trust into the provider or operator of an IMA depends on the individual. One factor is widely being regarded as enhancing the user's trust: The possibility to choose whether or for what contexts the IMA should be only located in the user's area and when a remote proxy would be preferred in a specific situation.

The advantages of offering identity management services external to the user's software or hardware client are obvious: This centralised approach means that only these central servers have to be maintained instead of organising a huge helpdesk for managing user support. What is more, the central servers' system environment is homogenous whereas a user-oriented application should be compliant to all relevant platforms, e.g., depending on operating systems (like different Microsoft Windows versions or one of several different Unix kernels), on programming languages respectively program execution environments (like different Java versions) or on various user interfaces. Not only the number of platforms causes a much higher effort for the IMS providers, but also individual user problems caused by interface problems or side effects with any IT component installed on the user's device.

Certain security requirements can be solved more easily in centralised services, e.g., daily backup, installing security patches on a regular basis, virus and malware protection, and other measures for safeguarding the IMS and the users' data. Technically, the user's data can be stored much safer on a server provided by professional IT staff of a provider than at home. However, as discussed, this requires the user to trust his provider to a larger extent or to apply additional safeguards, such as legal protection.

On the other hand centralised IMS are an attractive target for attackers because they concentrate valuable personal data and are a single point of attack for transactions.

IMS providers will need to maximise their profit and may sometimes choose to do so at the expense of security. Or the business model for their service might require that users give consent to processing of their personal data stored at the centralised IMS provider database for profiling or marketing purposes.

## 5.3 Identity Handling

Other dimensions are related to the way of identity handling in the IMS.<sup>196</sup> Many of these properties are also mentioned in [Art. 29 DPWP 2003], cf. the Annex.

### 5.3.1 Centralised vs. Federated Identity

In general we can distinguish between centralised identity and federated identity (and centralised and federated identity management):

- Centralised identity means that users and providers enrol with a central IMS provider which issues unique (global) identifiers (cf. Figure 85). The central IMS provider acts like a single gateway for the user's management of identities, e.g., in a single sign-on scenario the authentication of a user is performed by the central IMS provider. Because of the single point of control the system is easier to maintain, it means less effort in user support, and it is cheaper. Disadvantages are possible breaches of security and privacy requirements, because the systems concentrate personal data of the users, which enables the provider itself and possibly other parties to monitor the users' behaviour. The centralised concept puts big responsibilities on the providers, which should guarantee a high level of security and privacy.

---

<sup>196</sup> As discussed on the Workshop on Identity Management in Communication, European Academy for Freedom of Information and Data Protection, Berlin, Germany, 6<sup>th</sup> May, 2003.

- 
- Federated identities do not work with a single IMS provider. This category comprises both solutions with multiple IMS providers and implementations of user-side identity administration. As there is not one unique global identifier and no concentration of personal data outside the user's scope, users have (more) control over what personal data they share with whom.<sup>197</sup> The different service providers have control over user profiles, as far as they get to know them. For interoperation, standards of protocols and interfaces are required, such as in Liberty Alliance. The lack of centralised control may lead to inconsistencies of data. Federated identity management puts bigger responsibilities on the user and can mean more effort in user support.

### 5.3.2 Self-Authentication vs. External Authentication

As explained in Chapter 1.1.3, self-authentication means that the user himself or herself establishes a linkage between two of his messages or one message and a generated certificate. In this case no additional third party needs to be involved. External authentication requires an additional party to link the user's message to a proof of authorisation, such as a certificate [cf. Pfitzmann/Waidner/Pfitzmann 1990/2000].

A typical example of self-authentication is sending PGP-signed e-mails with user-generated keys, but using no additional party to prove his or her identity. Showing an identity card to prove one's name already comprises external authentication. The same applies for electronic signatures where a certification authority or PKI checks the identity information and then manages the link between the name and the public key.

The difference between self-authentication and external authentication is important when discussing the use of digital pseudonyms and the question when an application requires the use of third parties to authenticate externally the pseudonym and under what circumstances the application can do without (cf. Chapter 2.3.13).

### 5.3.3 Number of Identities per Person

The larger the number of identities per person, the more degrees of freedom the user has in identity management, resulting in both a higher degree of privacy (because of the potential for unlinkability) and higher complexity in use. In some IMS, users are not encouraged to use more than one identity per person, but these systems expect only one identifier and data set, e.g., the user's e-mail address.<sup>198</sup> Others offer a small set of pre-defined roles, which represent the user's identities. In certain systems, in principle any number of user identities can be created and managed.

### 5.3.4 Global Identity vs. Partial Identity

A context-spanning use with a globally unique identifier characterises the global identity, whereas partial identities are specifically used restricted to a role and/or communication partner (cf. Chapter 2.3.2).

### 5.3.5 Transfer of Credentials

Although today's IMS do not offer the transfer of credentials (cf. Chapter 2.3.2) from one pseudonym to another, this may be an important feature for a privacy-enhancing IMS because this provides unlinkability.

---

<sup>197</sup> If the system supports that service providers share their profiles, this is probably out of the user's control.

<sup>198</sup> Which may not be very anonymous.

## 5.4 A Common System Design: Infomediaries

An infomediary is a web site that provides specialised information on behalf of producers of goods and services and their potential customers. The term is a composite of information and intermediary. John Hagel and Marc Singer have defined infomediaries as "brokers or intermediaries that help customers to maximise the value of their data" [Hagel/Singer 1999]. This means infomediaries are information brokers that assist customers to articulate their determinations by protecting personal information against abuse and by disclosing personal data only with the customer's specific permission. The customer of an infomediary will have the choice either to remain anonymous or to allow his profile and his personal data to be given to vendors or direct marketers [Dumortier 2002: 28].

Infomediaries collect detailed information from their customers about their preferences in order to be able to find the web sites that suit them best [cf. IWGDPT 2000]<sup>199</sup>.

The architecture of infomediaries again is client-server based. As users of infomediaries choose to reveal certain personal data and define appropriate policies, they are presumably more aware of potential privacy risks resulting from the use of the service.

## 5.5 A Privacy-Enhancing IMS Architecture

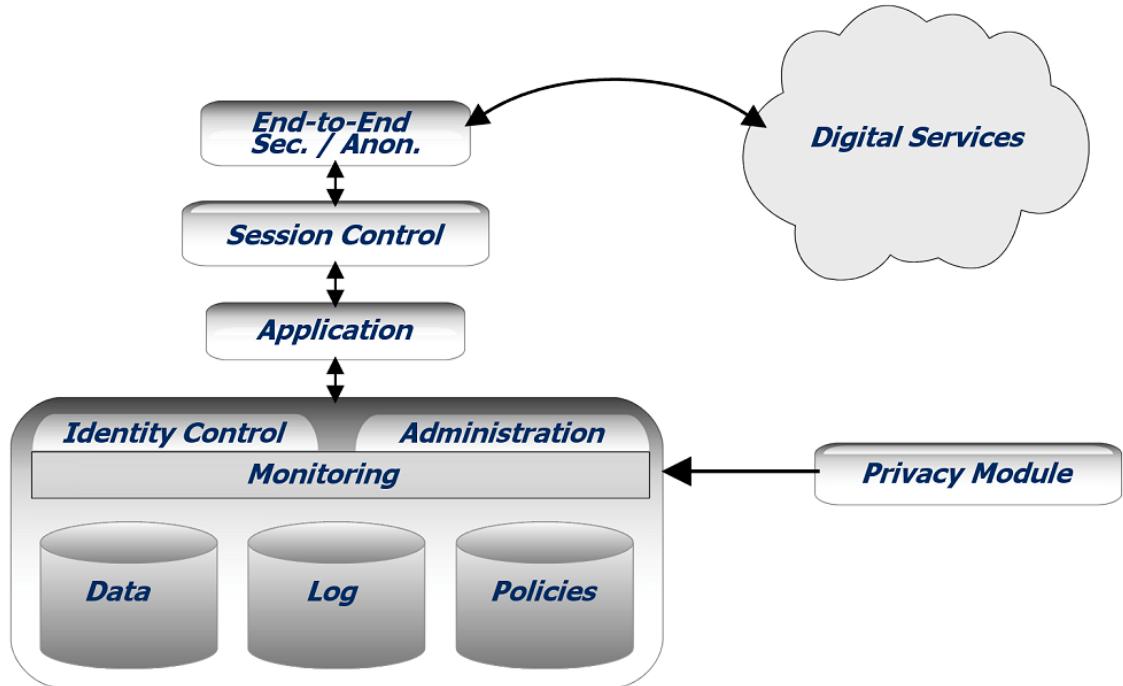


Figure 87: Architecture of a Privacy-Enhancing IMA

This conceptual architecture, which is being discussed in the EU project PRIME – Privacy and Identity Management for Europe, works both on user and server side [Hansen/Rost 2003]: Three databases store personal data, log files and policies. A monitoring component keeps track of all transactions. During communication sessions, the identity control is responsible for representation, handling and choosing the appropriate identity. Otherwise access is possible by the administration component. A privacy module can give input on privacy information data, which may influence the behaviour of the system and help the user in appropriate estimation of privacy risks.

<sup>199</sup> [http://www.datenschutz-berlin.de/doc/int/iwgdp/info\\_en.htm#nr3](http://www.datenschutz-berlin.de/doc/int/iwgdp/info_en.htm#nr3).

---

## **5.6 Summary**

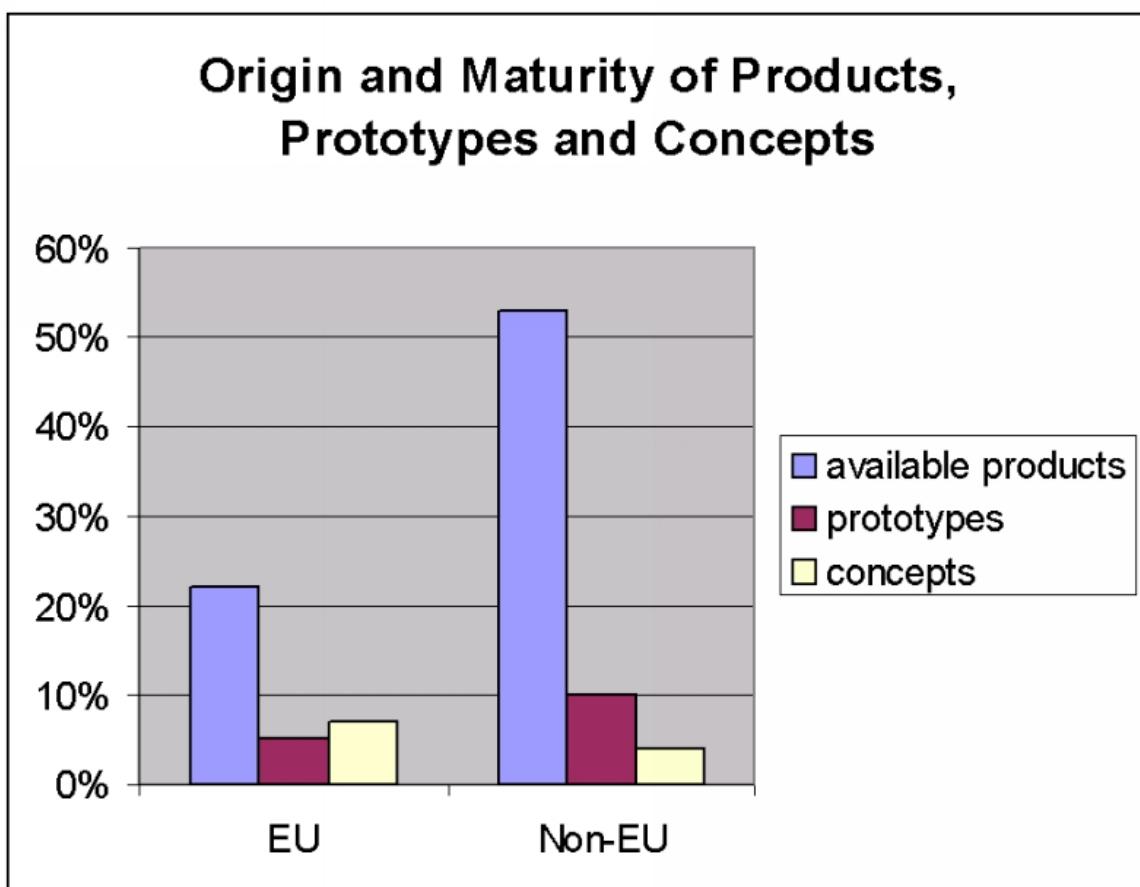
There are different IMS models and architectures, but for roughly estimating privacy, security and trust level, the appliance of only a few main criteria is sufficient. Different ways of integrating IMA in applications, different trust zones, and some properties of identity handling can be used to categorise IMS. These criteria could be additionally to the grid of attributes, proposed in Chapter 4.1, taken into account for future evaluation of IMS and IMA.

Additionally two models are highlighted which have not been presented in the previous Chapters: Infomediaries as a business and technological models and a component-based architecture of a privacy-enhancing IMA which fits both for client and server.

## 6 [CHAPTER F: EU CAPACITY]

### 6.1 EU Capacity

As described in Chapter 3, many identity management prototypes and products exist, being developed in various countries (cf. Figure 88). Many manufacturers of available IMA are based in non-EU countries such as the US. On the other hand in the field of identity management concepts and prototypes there is a focal point in EU countries. These IMA are often not available on the market yet, but compared to the standard US IMA they have stronger focus on taking legal and social criteria into account, e.g., striving to implement privacy protection legislation and other legal obligations, e.g., integrating electronic signatures or other technologies. Despite the availability and distribution of IMA from the US, the specific value of identity management as such is yet to be acknowledged and its paradigm is still fuzzy. The EU should be aware that next few years will provide the suitable time frame for establishing standards for IMS. It should take a leading role in this process.



**Figure 88: Comparison EU vs. Non-EU Activities on IMS (from Chapter 3)**

To promote the implementation of IMS concepts into applications and to ensure the utilisation of European know-how, diverse strategies could be followed in combination:

#### 6.1.1 Developing the Regulatory Frame

The elaboration of the legal basis in Chapters 1.1.2 and 1.2.2 has shown the liberal concept in the current legislative framework: In principle, anonymity and identity management are allowed and not prohibited, in some cases, these properties are sometimes even demanded.

---

In the on-line world this liberal approach should be maintained; especially the use of pseudonyms should be promoted rather than restricted, in order to allow in the digital environment the same degree of freedom recognised by liberal constitutions also in the digital environment. It is at least contradictory to expect that law enforcement at cost of freedom will produce better results in the digital environment than it has done (and does in some illiberal societies) in the physical environment.

The fact that a pseudonym is not forbidden, does not grant its relevance and validity if used in civil law transactions. Anyway there is no question for the jurisprudence that a contract closed between two parties is valid even if one of them was using a fantasy name or the name of another person. There are anyway exceptions, where the true identity of each party is essential, like the marriage and the recognition of paternity or maternity. Even in testamentary deeds it is not necessary to reproduce in full the administrative identification elements of the heirs: Pseudonyms (nick-names) are generally accepted as valid identifiers, as far as not inherently ambiguous.

The support of data minimisation techniques to achieve anonymity and pseudonymity is also a requirement for the deployment of PET, which is a stated objective of the Commission.<sup>200</sup> Although the driving principles behind the concept of PET can be derived from the Directive 1995/46/EC, it is mostly interpreted only from the data security point of view because PET criteria are not described in detail. Furthermore, incentives to really develop and use PET are missing in the Directive. Examples in, e.g., German law show that PET criteria are explicitly identified and therefore can be seen as objectives of technology design.<sup>201</sup> This could be a model for European law.

It is not sufficient to only lay down identity management principles in law. For instance, the Electronic Signature Directive 1999/93/EC already comprises a paragraph on pseudonyms<sup>202</sup> which is also implemented into national law, but nevertheless only very few pseudonymous signatures have been issued yet. Thus, European legislation on data protection and identity management should be enforced, so that real pseudonymous use is offered.

Additionally other incentives, such as harmonised Privacy Seals for privacy-compliant systems, should be developed. Regulation and co-regulation should complement one another.

### **6.1.2 Strengthening Leadership in Specific Technologies**

The European Union should expand its capacity in the field of chipcard technology and digital signatures, which are key enabling technologies for identity management. The same applies for anonymous credentials. European "I-centric" or other personalisation technologies, which do not consider typical identity management functionalities yet, should be enhanced in that way, e.g., for providing pseudonymous use or role management.

---

<sup>200</sup> Commission of the European Communities: First report on the implementation of the Data Protection Directive (95/46/EC); Report from the Commission; Brussels, 15.5.2003, COM(2003) 265 final; Luxembourg: Office for Official Publications of the European Communities, 2003.

<sup>201</sup> German Teleservices Data Protection Act (1997/2001):

§ 4 (6): "The provider shall make it possible for the user to utilise and pay for teleservices anonymously or under a pseudonym if this is technically possible and can be accomplished at reasonable effort. The user shall be informed of this possibility."

German Federal Data Protection Act (2001), § 3a: Data reduction and data economy:

"Data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for aliasing and rendering persons anonymous, in so far as this is possible and the effort involved is reasonable in relation to the desired level of protection."

<sup>202</sup> § 8 paragraph 3 Electronic Signature Directive 1999/93/EC: "Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name."

It is both in national and in Europe's regional interest, as well as in the interest of each user or service provider to use trustworthy IT systems.<sup>203</sup> Responsibility for data processing in ICT is impossible without control over the system and its design. This of course is crucial for critical infrastructures, but also for PKI and other trusted third parties, who are expected to sincerely provide for security of their IT systems. The same accounts for all e-commerce or e-government applications. Remedy can be achieved by building provably trustworthy hardware and software systems. Although no single state can finance this development alone, a common approach of all or a majority of EU member states could be successful, e.g., by using existing open source systems, enhancing them, and providing a defined way of evaluation, review, and maintenance [cf. Hansen/Köhntopp/Pfitzmann 2002].

### 6.1.3 Cultivating Market Niches

Although IMS are important in all kinds of digital communication and most people would expect e-commerce solutions at first, this market may not be the first choice for the more sophisticated IMA developments in Europe as competition is tough and margins are thin: It is too risky to reduce margins through investment in technology that will make transactions more transparent, but also therefore more complex. Instead of competing heads-on against rivalling technologies, the exploration of market niches for identity management services for employees in teleworking and collaboration, i.e., business-to-business applications or role management within a business may provide a feasible alternative in order to grow the market for IMA.<sup>204</sup>

One main driver could be the separation of private and professional lives for teleworkers at home: identity management would be introduced by the company for mainly professional purposes, but the employee may profit from the tools and methods also in private life. Additionally, e-government systems, which are currently being designed, should be evaluated for their potential in supporting identity management for the ordinary citizen. Here the compliance to legacy systems is of highly important. All these applications have in common a desired higher degree of assurance, which is not automatically achieved on the Internet.

Probably a trust infrastructure provided by a trusted third party could be the first environment where identity management will thrive. Such an infrastructure can be considered trustworthy provided that:

- a) It is a one-purpose enterprise, sustained only by revenues generated by the identity management;
- b) Its (security) policy is openly declared, assessable and adequate to the task of providing confidentiality and trustworthiness of the information;
- c) Its technology is open and transparent, assessable and adequate to the task of providing confidentiality and trustworthiness of the information;
- d) The liability model provided is adequate: Either the company has a significant patrimony, or the management (and the shareholders) are personally responsible for each confidentiality breach (like professionals are, if they breach their contractual obligations).

---

<sup>203</sup> From the European Parliament Resolution on ECHELON, Minutes of September 5, 2001: "Measures to encourage self-protection by citizens and firms[...] 29. Urges the Commission and Member States to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software;

30. Calls on the Commission and Member States to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes;  
 31. Calls on the Commission to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the "least reliable" category [...] (<http://www2.europarl.eu.int/omk/OM-Europarl?PROG=REPORT&L=EN&PUBREF=-//EP//TEXT+REPORT+A5-2001-0264+0+NOT+SGML+V0//EN>, mirrored at <http://cryptome.org/echelon-090501.htm#Minutes>).

<sup>204</sup> Note that this is no contradiction to the user-oriented view of this study: This paragraph focuses on the user as employee or other member within an organisation who works together with other team members, possibly from other organisations [cf. Figure 9], as sketched in modern working models. The organisation could provide IMA for their members, and if the IMA works outside the organisational context, too, the additional application contexts would support the wider distribution of identity management functionality.

---

One European project seems to be heading in this particular direction, namely EASET – European Association for the Security of Electronic Transactions, launched by European notaries<sup>205</sup>.

In all these areas, experiences could be collected which lead to more standardised and distributed multi-purpose IMA.

#### **6.1.4 Funding**

Privacy and identity management is one of the topics where research and technological development can be funded by the Commission, e.g., the project RAPID – Roadmap for Advanced Research in Privacy and identity management in its Fifth Framework Programme for Research and Technological Development. In the Sixth Framework, first call, "Privacy and Identity Management" is among the topics which may be funded in an Integrated Project and a Network of Excellence [Hansen et al. 2003].

Further projects address related topics, such as privacy technologies, and have been partly financed by the Information Society Technologies (IST) research programme:

- DRIVE – Drug In Virtual Enterprise<sup>206</sup>;
- MAFTIA – Malicious- and Accidental-Fault Tolerance for Internet Applications<sup>207</sup>;
- PAMPAS – Pioneering Advanced Mobile Privacy and Security<sup>208</sup>;
- PISA – Privacy Incorporated Software Agent<sup>209</sup>;
- PRIDEH – Privacy Enhancement in Data Management in E-Health<sup>210</sup>.

Other European programmes have supported projects like SEMPER – Secure Electronic Market Place for Europe<sup>211</sup>, CAFE – Conditional Access For Europe<sup>212</sup>, or SEISMED – Secure Environment for Information Systems in Medicine<sup>213</sup>.

Additionally topics like "Smart Government" or "e-Democracy" may touch identity management-related issues.<sup>214</sup>

#### **6.1.5 Standardising Identity Management**

The standardisation of identity management functionality is important to ensure that IMA can work together with each other and with other systems as well. It would be best to develop IMA in a way so that their new potential can be used, but that they are still compliant to legacy systems. Being embedded in the European legal system and the European application and culture context, functionality should be harmonised in accordance. This covers among others pseudonym properties, integration of third parties, interpretation of logs and ways for context detection, user interface, default privacy preferences and communication styles. This should culminate in the development of world-wide standards for an Identity Management Protocol Set.

---

<sup>205</sup> Cf. Chapter 2.1.6.2.

<sup>206</sup> <http://www.e-mathesis.it/Drive/>.

<sup>207</sup> <http://www.newcastle.research.ec.org/maftia/>.

<sup>208</sup> <http://www.pampas.eu.org/>.

<sup>209</sup> <http://www.pet-pisa.nl/>.

<sup>210</sup> <http://www.prideh.custodix.com/>.

<sup>211</sup> <http://www.semper.org/>.

<sup>212</sup> <http://www.semper.org/sirene/projects/cafe/>.

<sup>213</sup> <http://www.semper.org/sirene/projects/seismed/>.

<sup>214</sup> <http://www.cordis.lu/ist/ka1/administrations/projects/clustering.htm>.

The success of the EESSI standardisation process for the technologies needed for the qualified electronic signatures<sup>215</sup>, allows to consider it a possible model for future legislative framework for the ruling of innovative technologies. In fact there is a fundamental contradiction between the rule of law and the rules of code [Lessig 1999], between national rules and global rules. In order to tame the contradiction, the only success so far has been international standardisation (IETF<sup>216</sup>, EESSI<sup>217</sup>, ETSI<sup>218</sup>, etc.). For the success of such an approach, a clear role distinction has to exist: Legislation provides the "what", i.e., the goals (like security, transparency, openness, consumer protection, privacy protection, etc.); industry, academia and consumer led standardisation provides the "how", i.e., the technical and practical solutions that can cope with the goals set by the legislator.

The currently best open security assessment criteria available are the Common Criteria [ISO15408 1999]: It is an open security assessment scheme to which states can apply. To be admitted a national security assessment scheme has to be put in place, providing adequate security assessment regulations and a national agency with the proper competencies to carry out security evaluations and to accredit security evaluation facilities.

From the security and privacy point of view, which are of utmost importance with respect to IMS, well-known evaluation processes should be adapted to identity management requirements. For instance, the Common Criteria which already contain anonymity and pseudonymity properties in the privacy functionality class could be extended by transparency or user empowerment criteria; protection profiles for different IMS types could be developed.

It is certainly possible that in such a co-regulative process specific inadequacies of the legislation become evident: in this case a revision process of the (European) legislation shall be possible. Accordingly Article 12 of the Directive 1999/93/EC provides a time frame for review of the directive. Such a review process has recently been started with the appointment of an expert group that has to provide information to the Commission in order to real need to review the directive. First results of the experts work are expected in September and will be presented at ISSE 2003 in Vienna.

Anyway the key technology for any form of IMS and IMA is the secure electronic signature, of which the qualified signature is the paramount example. It is not a coincidence that the security of the most relevant elements of a PKI (signature creation devices, key generation devices, certificates managing devices) are submitted to Common Criteria Security evaluation, in order to be compliant to the European Directive on Electronic signature. Neither is it a coincidence that all this complexity has harmed deployment of the electronic signature. The cost of this essential infrastructure of the information society cannot be born by private industries. Only if a monopoly were to be granted to the companies that build such an infrastructure (like it was the case with railways, electricity and telecommunications in most European nations), could they expect returns on investment that would make such investment attractive.

---

<sup>215</sup> The first fundamental technical standards for the technical security of the qualified signature have been published in the Official Journal of the European Communities the 15<sup>th</sup> July 2003, L 175/45. There is so the presumption that:

- a) secure signature creation devices are compliant to the security requirements of the directive, if compliant to the security assessment criteria laid down in the Cen Workshop Agreement (CWA) 14169
- b) qualified certificates are managed in a secure manner, if the infrastructure managing them is compliant to the security assessment criteria laid down in CWA 14167-1, and CWA 14167-2

<sup>216</sup> Internet Engineering Task Force, that has produced the open standards that are ruling the Internet. A full voluntary, not government backed standardisation activity ([www.ietf.org](http://www.ietf.org)).

<sup>217</sup> European Electronic Signatures Standardisation Initiative: an initiative launched and partially funded by the European Commission, but led by a Steering Group composed by individuals working without any compensation. Within EESSI two workshops have been established:

- 1) Cen-ISSS E-Sign WS (<http://www.cenorm.be/isss/workshop/e-sign>), and
- 2) ETSI ESI TC (<http://www.etsi.org/esi/el-sign.htm>, or <http://portal.etsi.org/esi/el-sign.asp>), both with about three dozens of active (non funded) participants and partially funded experts teams.

<sup>218</sup> European Telecommunication Standardisation Institution: an official European standardisation body, whose participants are governmental organisations and private companies. ETSI has produced with the same methodology of the EESSI WSSs the GSM specification, that has become the world-wide most used specification for second generation mobile phones.

---

As however monopolies are legally permissible and politically sustainable only in exceptional cases, according to the European legislation on single market and competition. Therefore there is the case for a central role of governments in subsidising and supporting the creation of trustworthy PKI in Europe as an essential asset for competitiveness in the information society of the next 20 years.<sup>219</sup>

### **6.1.6 Building Infrastructures**

As multilateral identity management solutions rely on technological and organisational infrastructures, it is necessary to provide these technologies and services. At least for e-government applications the member states may be willing to provide the appropriate infrastructure, possibly comprising identity management functionality, but at least offering the possibility to enhance the systems according to identity management as it is expected to be state-of-the-art in the near future.

Incentives for business to help building these infrastructures and offering necessary services are necessary. The member states could, e.g., grant tax deductions or other privileges for supporting this kind of infrastructure.

### **6.1.7 Gaining Awareness**

Although people intuitively manage their identities in ordinary lives with face-to-face contacts in the off-line world, they are not used to the opportunities and risks related with digital identity in the on-line world. Thus, education is needed, at best already in schools or even earlier. The Commission could support this with educational campaigns for ICT and media competency in general and more specific for privacy- and identity-related topics.

The project eAWARe<sup>220</sup>, supported by the Directorate General for Research of the European Commission, aims to educate the everyday Internet user about on-line risks and the steps users can take to protect themselves. This project can be seen as a first step in the direction mentioned. eAWARe reaches out to the public through local events across Europe. However, this approach has to be accompanied by training and education in schools as well as courses and workshops for other target groups. For example in e-learning projects, modules for privacy, security and identity management could be developed and provided for free for educational purposes.

### **6.1.8 Exporting EU Know-how**

The building blocks for IMS, which fit in the European context, are mostly available, although some are still at the concept or prototype level. The logical next step is sharing and export of knowledge, which can be done through the established channels of the technical and scientific community, e.g., white papers. Ultimately, this should lead to the development of standards and products. Also existing products should be monitored whether they fulfil the criteria, which are important for European users. As mentioned in Chapter 4.2.2, the European Article 29 Data Protection Working Party has already given a first statement with a critique of the Microsoft Passport system [cf. Art. 29 DPWP 2003]. Microsoft has accepted the critique and has worked out a roadmap when to adjust their system to which requirement of the working group in the next year [cf. PS 2003]. Another example is the Safe Harbor Initiative.<sup>221</sup> Both are good examples for the influence stream of European privacy requirements on distributed systems.

---

<sup>219</sup> This is the approach taken by many Asian states, in particular Japan. See <http://www.jnsa.org/mpki/> and <http://www.ietf.org/proceedings/02nov/slides/pkix-5.pdf>.

<sup>220</sup> <http://www.eaware.org/>.

<sup>221</sup> <http://www.export.gov/safeharbor/>.

## 6.2 Summary

The current posture of the European Union in the field of identity management is quite favourable in the academic and research sector, but there is a need for transfer of the existing intellectual capital into real-world applications. In contrast to most currently available IMS, many of the concepts or prototypes from European institutions meet the requirements of assurance or privacy, which are set in the harmonised legal framework of the EU. The EU should profit from its strength in diverse areas and take over a leading position in developing IMS, which implement security and privacy protection criteria, helping the user to gain sovereignty over his or her personal data.

This Chapter elaborates EU capacity, e.g., in the regulatory framework which already is suitable for identity management and can be further developed to support IMS even more. Key enabling technologies with European background are e.g., chipcards or digital signatures. The EU should combine their ICT development power to design and implement on their own in crucial points. Because of – among other reasons – protection of critical infrastructure, the EU should preserve some autarky and invest in independent developments of trustworthy ICT.

Market niches are identified where specific EU-developed IMS could be implemented. Since the business model is not yet clear for all concepts and since some fundamental research is necessary, funding programmes should help in developing IMS and interdisciplinary working out solutions. In fact, two EU-funded research projects, PRIME – Privacy and Identity Management for Europe and FIDIS – Future of Identity in the Information Society, start within the next months and are expected to soon present their first results. Both projects will contribute to standardisation, one of the key areas for ICT in information society. This could help building the appropriate infrastructures. Here the member states should be encouraged to give incentives such as tax deduction.

Awareness, education and training are other areas where all member states have to invest in the future. Collaboration in developing e-learning modules could reduce costs and set common standards. All action lines on ICT awareness should also add security, privacy and identity management issues.

Finally the EU could export know-how in the field of identity management as it is already done in the data protection area, e.g., via the Article 29 Data Protection Working Party with their Working document on on-line authentication services [Art. 29 DPWP 2003].

---

## **7 [CHAPTER G: VISION AND OUTLOOK]**

This Chapter first describes possible roadmaps for IMS technologies. Afterwards an outlook is given.

### **7.1 Roadmap**

In this Section we describe the RAPID<sup>222</sup> roadmap on privacy and identity management of the RAPID project and develop an approach to extrapolating current IMS technology threads and trends.

The RAPID project has already developed a roadmap on privacy and identity management, focussing on applied research and dealing with time frames of 0-3 years, 3-5 years and 5-10 years. The focus of this study differs from the RAPID approach as we concentrate firstly on market penetration of IMS and secondly on technical maturity of IMS concepts and applications. We sketch our roadmap in a longer term, elaborating possible future developments until 2020.

#### **7.1.1 RAPID – An Existing Roadmap on Privacy and Identity Management**

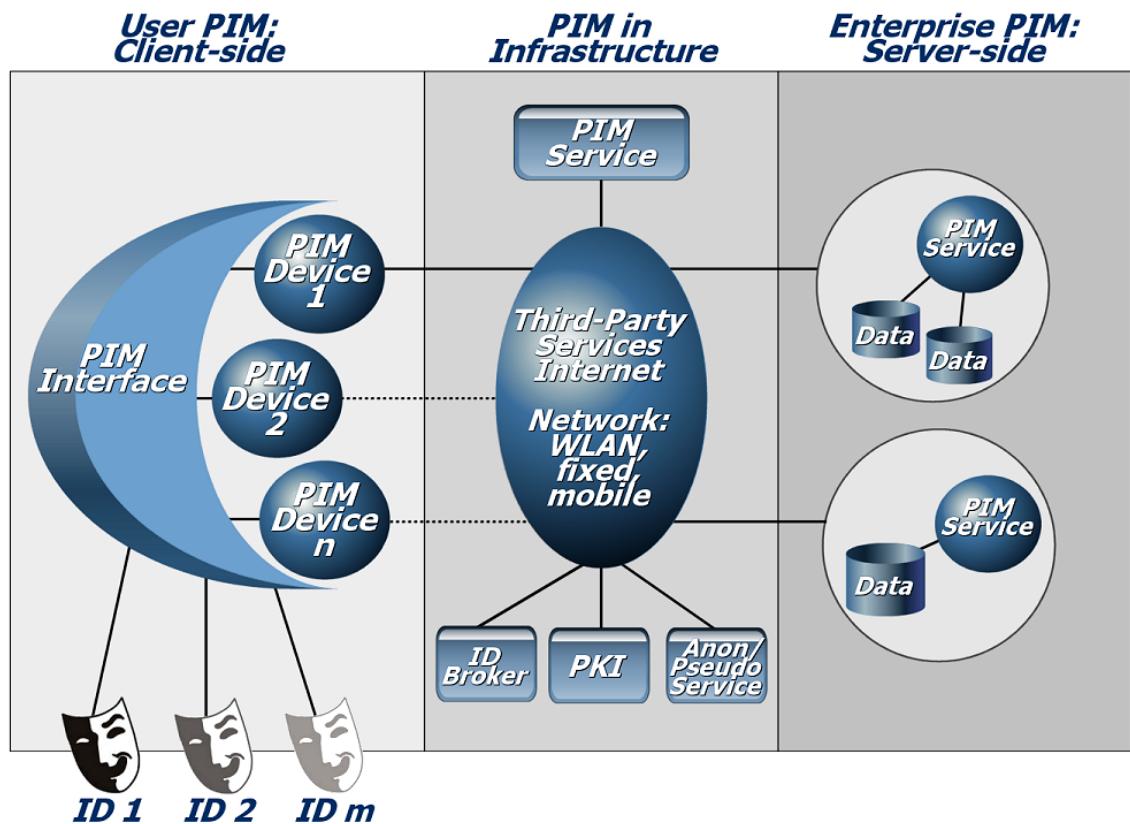
The RAPID project has been working since 2002 on developing a strategic roadmap on privacy and identity management (PIM). It focuses on applied research in this area. There are different streams on PIM research and technological development, which produce their own roadmaps:

- Research for socio-economic aspects (including new computing paradigms)
- Research for legal aspects
- Research for multiple and dependable identity management
- Research for PET for enterprise
- Research for PET in infrastructure.

The results are integrated into an "overall roadmap". The preliminary results are quoted in the Annex.

---

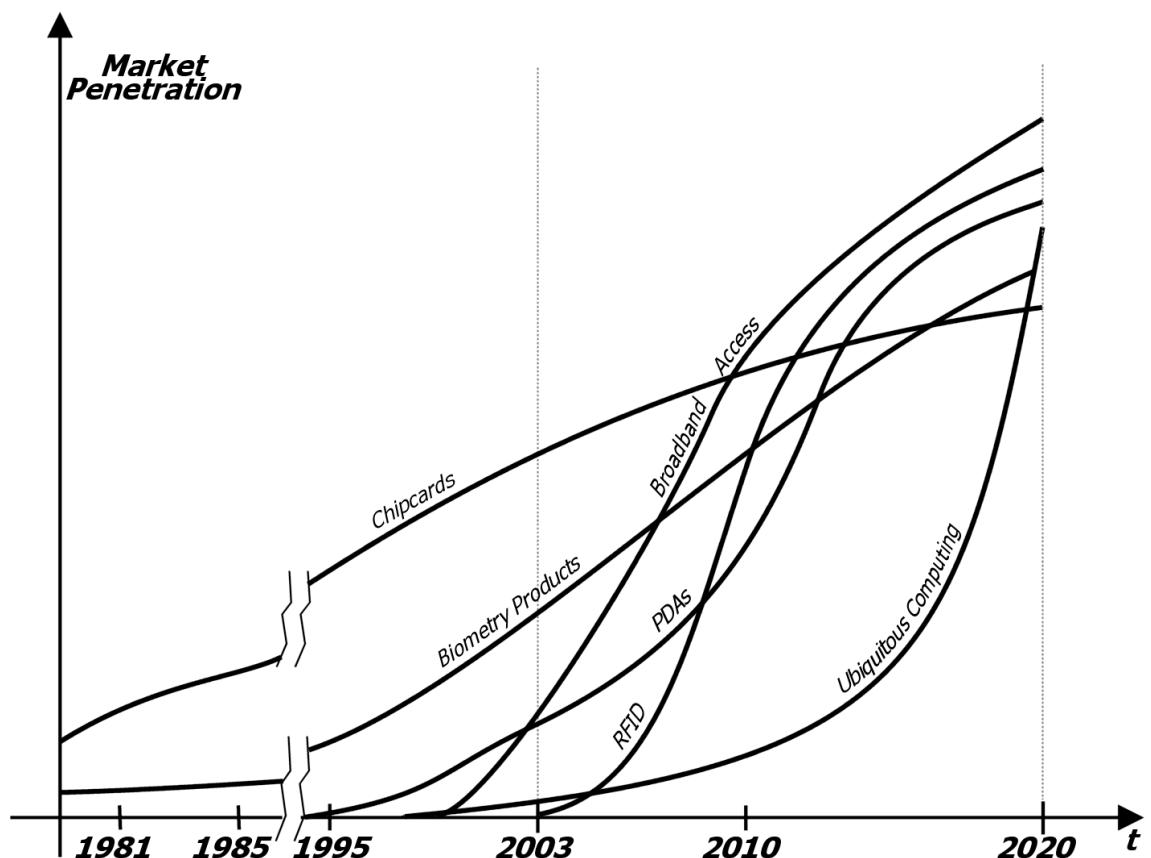
<sup>222</sup> Roadmap for Advanced Research in Privacy and Identity Management.

Figure 89: PIM in RAPID's Vision<sup>223</sup>

### 7.1.2 An Approach to an IMS Roadmap

The adjustment of all identity papers and the transfer of their results to an electronic medium is being continued. The communication with different organisations via Internet becomes the normal case. The media (CPU/memory/interfaces) become smaller and more efficient. Within this transfer, one question repeatedly comes up: How many different identification requirements by different institutions can be standardised and consolidated? An at least rudimentary IMS is available and allows the user to recognise and select different pseudonyms for different communicative requirements.

<sup>223</sup> [Huizenga 2003].



**Figure 90: Roadmap: Market Penetration Techniques**

Biometric techniques for identification by physical attributes have hardly recovered from the relative disillusionment concerning their reliability that spread since the beginning of 2000. It still requires only small effort to outsmart, e.g., the scanners for face, fingerprint, eye, and of walk or handwriting identification. The industry's promises about the ultimate authentication system are unfaltering, though. The number of installations increases slowly but steadily. Pragmatically, the installations try to combine as many different approaches of biometrically covered identification to reduce the remaining residual risk. Customers have to deal with the responsibility risk (unnecessary examination and identification of persons and co-workers, fraud) politically, legally and economically.

Security in information technology has improved over the last decade along with the proliferation of information technology in business processes. The Business management has realised that they are existentially dependent on a reliable infrastructure and may face financial penalties if it fails to apply due care to safeguarding of IT-based business operations. Currently, there are however still indications for a solely cost driven instead of risk driven approach in corporations of all sizes. A broad range of technologies for the purpose of improving security and data protection is being deployed. Particularly, developments concerning the technical securing of access rights close to the core level of operating systems play a decisive role. At the same time, TPMs (Trusted Platform Modules) will have widely been established, particularly because TPM technology has already been integrated into the Intel LaGrande CPU. Operating System Components will make use of the cryptographic abilities TPMs offer, and Digital Rights Management (DRM) systems will make use of the operating system components. TPM technology and the mentioned operating system components are especially used by organisations as in combination they allow a simple and reliable control and monitoring of the processes within organisations.

As TPMs provide strong cryptographic functions, law enforcement agencies will demand backdoors. As this will fundamentally undermine the security value of TPM-based technology, less acceptance and therefore less market penetration is to be expected. At the current state the

market penetration of trusted computing components such as TPMs is not seriously predictable. Therefore it is not represented in Figure 90.

Ubiquitous computing is on the advance, the objects becoming more and more intelligent and communicative. By use of "Smart Dust", a descendant of particularly small RFID-tags (Radio Frequency IDentity: identification through smallest radio units), practically every object can be identified. They substitute the old barcodes in shopping centres. While around the year 2000, a Smart Dust particle disposed of a 4 bit address bus and a 3 kB RAM (of which 1,4 kB were used for the operating system) and had a range of approx. 10 to 100 metres, ten years later, these particles show the efficiency of a millennium PC, as far as the processing and sensorics are concerned. This is being transferred to bigger and more complex contexts. For example, the apartments become smarter, too. Devices respond to calls in a flexible manner, grocery suppliers are filling refrigerators automatically. Rooms containing people and technology identify and interact with their inhabitants in a personalised way.

### 7.1.2.1 Market Penetration of IMS

We will in the following consider three possible scenarios regarding the social penetration of IMA or the social acceptance of IMS respectively in the sense of a "background fulfilment"<sup>224</sup> [cf. Gehlen 1956]. Scenario A is the optimistic variant in which IMS are a radical success and experience rapid growth. Scenario B is the "conservative variant". All development takes longer than the minimum required time based on the maturity of the concepts, the first technical implementations and the social problem pressure. As examples for a similar development, one only needs to think of the reluctant use of e-Commerce, the low degree of usage of digital signatures and the relative unpopularity of PGP. Scenario C is a pessimistic variant. A disruptive event of some kind is stopping all conceptual, technical, legal and political development in the area of identity management. This scenario describes a world in which all conceptual elements of IMS are available and from a technical point of view only their integration is missing, however society is not accepting such systems.

---

<sup>224</sup> Originally "Hintergrunderfüllung".

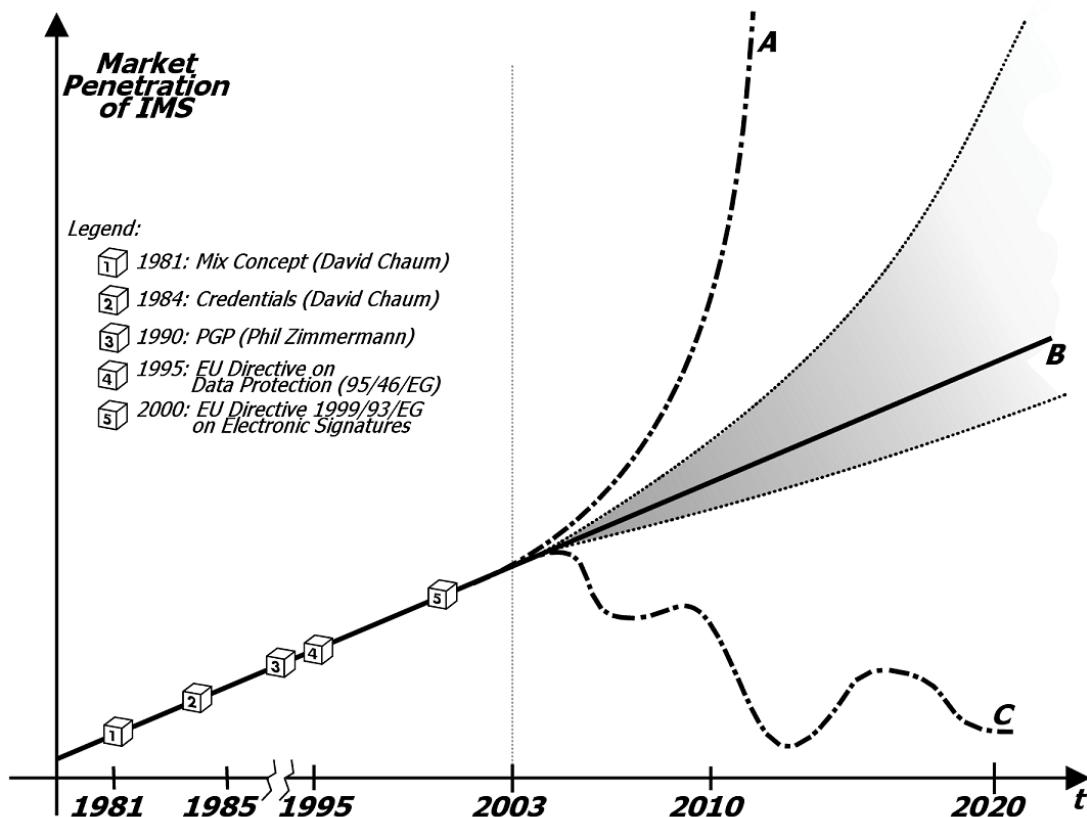


Figure 91: Roadmap: Market Penetration of IMS

#### Growth-Scenario (Scenario A)

First approaches to self-coherent IMA worthy of this name are being rapidly – i.e., over a period of two to three years – distributed to PCs in organisations and in the private sector of highly developed industrialised countries. A comparable example for the required speed and depth of penetration one would think of MP3-enabled music players or DivX-enabled video players.

Such a scenario is not unrealistic if

- IMA can ride on a wave of acceptance for other applications. In concrete terms, one would think of personal agents and location based services or an accelerated penetration of ubiquitous computing. These may spread more rapidly because they provide an immediately visible use and an obvious enhancement in comfort of use. With their spread, demand for identity management would certainly grow.
- IMA are technically easy to use, i.e., easy to install and configure and are available for a variety of operating systems. Ease of use can be assumed when IMA become integrated components of operating systems, similar to the amalgamation between Microsoft Windows XP and Microsoft Passport or web browsers.
- IMA are being supported by tabloid papers and if these were to promote identity management for campaigns sustained over a longer period of time, thereby promoting these applications to end users and stimulating further demand.
- IMA are being made mandatory by privacy law for the use in organisation.

### **Steady-State-Scenario (Scenario B)**

This scenario describes the continuation of the current development under the assumption of a slight market growth. None of the big promises, announcements or horror scenarios that were predicted along with the new quality of automation of socially relevant communication – e.g., with regards to ubiquitous computing, subcutaneous implementation of computer chips in humans (Kevin Warwick, [cf. Warwick 2002]), the electronic home (Bill Gates), electronic money, personal agents or the use of digital signatures in civic administrations – are being implemented explosively or over night. All of these new trends grow slowly, interacting with each other. The same will be true for IMA. Most of these new applications depend on the presence of tailored infrastructures whose feasibility and practicability clearly cannot be considered a proven fact at this point in time.

Nonetheless, it can be presumed that a massive use of digital signatures will have the largest possible effect on the social penetration of the other technologies. Digital signatures enable authenticity and non-repudiation of communication and actions to persons and organisations, so that the traditional approached to law and jurisdiction will not have to undergo substantial change. From this perspective, digital signatures support legal assurance in a traditional sense. Identity management could have a similar effect because it affects a multitude of other applications. It would be very useful to closely link a personal agent with identity management software, both of which are captured in the network of ubiquitous computing.

### **Regression-Scenario (Scenario C)**

Scenario C describes a case where unforeseeable but not improbable events with far-reaching consequences occur which could stem the growth of identity management for a longer period of time. Several such events can be imagined:

- The "crypto catastrophe". It could turn out that the crypto algorithm used by most applications for signing and encryption becomes instantaneously unsafe by a new process. A possible consequence would be the collapse of all legally binding, automated communication between organisations. If no quick replacement can be found (e.g., elliptic curves instead of RSA), not only the further use of IMA is inhibited, but also network-based, social communication at large. A solely legal regulation in order to sanction an attack on insecure crypto algorithms would probably be ineffective.
- The "political disruption" in the spirit of September 11<sup>th</sup>. This somewhat colloquially named category addresses the phenomenon that political organisations see themselves under pressure to elicit a quick and thereby imbalanced reaction to certain social events. From one moment to another, the government is successful in implementing a whole bundle of regulations restricting civil liberties over a period of only two months that it was unable to generate political consensus for in several years leading up to this day. A political-legal requirement can be phrased to prohibit anonymous communication over the Internet. Internet Service Providers find themselves legally obliged to protocol all connection data of their customers for the authorities' perusal. An effective identity management is hardly imaginable if there is no way for communication unmonitored by third parties. Identity management in so far is dependent on the presence of a civil constitutional order while on the other hand it serves to stabilise this order when it has been implemented. Another "political economic-related catastrophe" could result from a single vendor succeeding in establishing his own implementation of identity management as a monopoly and thereby as a quasi-standard.

We need to consider that a society that has survived a "social catastrophe" will likely react with countermeasures as soon as it becomes capable of them, which potentially will improve conditions beyond the status quo ante.

---

Possibly, only an "crypto catastrophe" will drive the development of stronger technology. Maybe a comparison with countries in which civil rights for the use of a sovereign, technically supported identity management weren't cut or suppressed will show their greater economic potential.

In modern society, the possibility exists that such disruptions can be avoided because in a dynamic society, alternatives are being developed alongside and thus are present before the catastrophe.

### 7.1.2.2 Maturity of Concepts and Applications for IMS

Thinking about David Chaum's concepts and their implementation we see that the gap between available concepts for performing secure and privacy-compliant technically supported communication and technical implementation in products is steadily widening.

Again, three possible scenarios about the relation between the existence of mature concepts and the maturity of technical implementation can be distinguished.

In order to give some background to this prognosis, the following tables shall give an overview on two key areas of technology for PCs and PDAs in 2010 [cf. Pfitzmann 2001a].

**Table 31: Prediction PC Mass Storage**

2010	Magnetic Hard Disks	Magnetic Disks	Optical Disks	Magnetic Tape Drives
<b>Capacity</b>	10,000,000 Mbyte	1,000 Mbyte	16,000 Mbyte	240,000 Mbyte
<b>Access Time</b>	0.005 s	0.03 s	0.02 s	20 s
<b>Dimension:</b> - Unit - Storage Media	"Cigar case" (Mounted)	"Cigar case" 90x93x3mm	"Cigar case" DVD	"Cigar case" DAT
<b>Price:</b> - Unit - Storage Media	200 DM [100 €] (Mounted)	50 DM [25 €] 20 DM [10 €]	200 DM [100 €] 3 DM [1.50 €]	1,000 DM [500 €] 50 DM [25 €]

**Table 32: Prediction Computer**

2010	PC	Pocket Computer (PDA)
<b>Command Size</b>	128 bit	64 bit
<b>Commands</b>	100,000,000,000	5,000,000,000
<b>Storage Capacity</b>	65,536 Mbyte	2,048 Mbyte
<b>Access Time</b>	0.000,000,000,3 s	0.000,000,003 s
<b>Cache Capacity</b>	256 Mbyte	-
<b>Access Time</b>	0.000,000,000,2s	-
<b>Dimension</b>	"Pizza Box"	120x80x10mm
<b>Price</b>	5,000 DM [2,500 €]	1,000 DM [500 €]

These prognoses encourage the assumption that the factors that are hitherto limiting ambitious technical development, such as storage and performance, will have less relevance in the future. In this model, conceptual or technical bottlenecks will no longer have an impact that could

inhibit social penetration and ubiquity of technologies offering qualitatively new functionality.

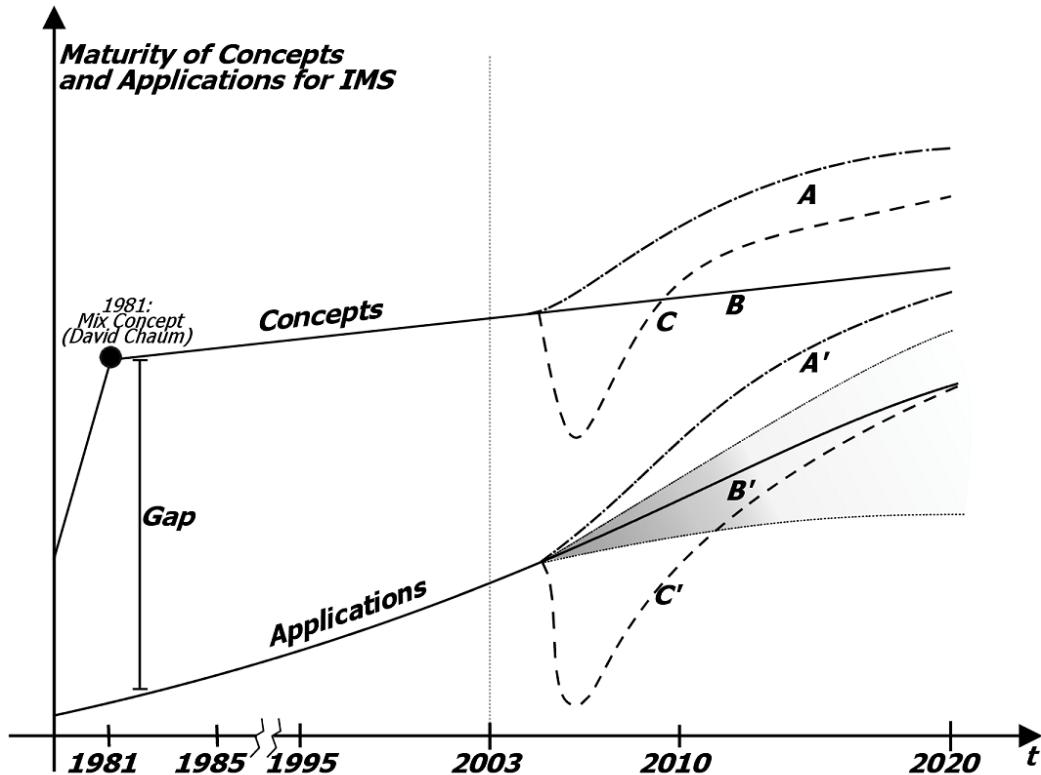


Figure 92: Roadmap: Maturity of Concepts and Applications for IMS

#### Better Concepts – better Applications (Scenarios A/A')

Important concepts in an immediate relation to identity management were developed ad hoc by David Chaum et al. over a very short period of time. These concepts (about anonymity, signatures, pseudonyms and credentials) are accessible, they have been stabilised and they are being permanently developed further world-wide. There is a potential for qualitatively new approaches, such as in the general context of quantum computers and quantum cryptography. This conceptual development was followed by the development of technical products narrowing the gap between concepts and applications.

#### Good Concepts – good Applications (Scenarios B/B')

These interrelated scenarios describe a situation where the concepts have been widely developed and no new practical development is to be expected. The implementation in products can be steadily performed, so that theoretical concepts and their implementation in applications follow increasingly faster to one another. Within this conservative estimation, two more detailed scenarios can be formulated. On the one hand, the implementation of concepts within application can be effected faster than was to be expected by extrapolation of past tendencies, so that the development follows line B'. Such a development could be the consequence of using digital signatures, so that these permeate society further than so far. On the other hand, it is possible that the current state of development of applications immediately related to IMS is practically frozen, because law, political intentions or market interests are directed against applications that are essential for the implementation of IMS.

#### Bad Concepts – bad Applications (Scenarios C/C')

This pair of scenarios highlights the possibility of sudden invalidation of concepts and algorithms required for IMS ("crypto catastrophe"), which would radically and immediately cripple functionality of applications based thereupon.

---

Thereafter, as the curve suggests, more mature concepts based upon increased scientific knowledge and will become available, and as a consequence more mature applications will be developed.

We advise to take these curves with a grain of salt. Their primary objective is to make alternatives for future development visible, so possible reactions can be evaluated in due time.

## 7.2 Outlook

Assuming that the European legislation will recognise and adequately regulate the individual right to pseudonymity and anonymity on open networks, enhancing and better specifying the provision of Annex I of the Directive 1999/93/EC (the first existing piece of European regulation recognising the right to pseudonymity), in the future each part of our individuality will be properly represented in the digital environment.

In the long term future not only various kinds of organisational communications will be standardised, but also how to manage one's identities. First of all, basic anonymity services will exist, which are available to everyone. Especially anonymity on the communication network layer will be a universal service. This is necessary to protect the identities of the communicating people or items and the communication links against observers because this information must not be used by unauthorised entities. All the same, the communication lines will be secured by end-to-end encryption as a default so that confidentiality and integrity of the content on the way through the network is guaranteed.

Furthermore, IMA based on the underlying anonymity services will be widely distributed. Some of them will be integrated in specific application software, some will be realised as multi-purpose IMA integrated in all kinds of communication systems, e.g., in a mobile phone, an Internet browser, or a PDA. All IMA will be compliant to a set of standardised Identity Management Protocols which among others enable the communicating partners to declare the requirements to and configurations of the use of partial identities, especially what pseudonym type to choose in which context. Those Identity Management Protocols have to be compliant to law. Legislation, accordingly, shall provide an accurate and sustainable balance between the rights of individual freedom and the needs of law enforcement.<sup>225</sup>

An appropriate infrastructure (that will need an appropriate regulatory framework disciplining quality assessment and liability of the service providers) will support the user's identity management, e.g., by a PKI, by various third party services, such as identity brokers, value brokers or delivery services, and by help in using and configuring the IMA. New business models will emerge. On one hand, there will be on-line help from Privacy Commissioners, other authorities or peers. We expect that already in school will pupils learn how to manage their identities with an IMA, as also some basic programming skills could become universal knowledge like the ability to read, write or calculate.

Usability of the IMA will be good, even for untrained users. Everybody will be aware of the default configurations of their IMA, which will be compliant with privacy requirements. Some users will heavily use the expert mode and all sophisticated functions, but most will consider the default configurations as sufficient for their needs, or will resort to some "Identity Protector"<sup>226</sup>. Many people will store their personal data in their IMA located at the user's side. The security level of client computers with specific trusted computing areas will be much higher than in 2003.

---

<sup>225</sup> Cf. Chapter 2.1.2.2 (Identity Protector).

<sup>226</sup> Cf. Chapter 2.1.2.2.

Where there is no established trust and security infrastructure, for data, which the users do not consider too sensitive, IMS providers will act on behalf of the users. However, most third parties who help the user with his or her identity management offer either only operational and non-semantic services or they are integrated in the workflow of a specific application and act there as a party trusted by all communication partners<sup>227</sup>, as far as they will be single-purpose entities, entirely dedicated to the identity protection and management. IMS providers who offer centralised services for managing personal user data, meanwhile will have added user-side-oriented services to their portfolio. For convenience reasons or because of limited resources under specific circumstances the centralised services will be preferred, but many users will decide consciously when to use the centralised and when the user-side solution. Companies and some communities may offer IMS functionality to their members.

The use of pseudonyms will be accepted for the majority of applications, as is the case today in the majority of small transactions carried out in the physical environment. For many scenarios it is sufficient that the user generates the pseudonyms and certificates by himself or herself. In others, the public service will issue a pseudonym, e.g., on a chipcard, in many cases together with digital authorisations which may consist of anonymous credentials. Especially official documents such as passports, driver's licences, social security cards and police certificates of good conduct will still be issued by public administration. Furthermore, business will issue pseudonymous certificates as digital customer cards, which can be used in communications with companies or company consortiums.

IMA will be used as a matter of course in handling the manifold accounts of a person. Role management will be a favourite application, e.g., in order to separate professional from private lives, incorporating both management of authorisations and reachability management functionality. In these cases the employers will fund the use of IMA and train their employees. In private lives, people will have to pay for the anonymity and identity management services. Certain services may be subsidised by advertising up to the point when they are free to the user. People will be able to decide explicitly whom to disclose what data. As a result, they may not always chose the solution offering the biggest privacy, e.g., services will be cheaper if more accurate personal data is disclosed.

New technologies, such as user controlled software agents, will promote self-determination. New technologies such as ubiquitous computing will add another component to today's identity management as each object exhibits its a certain identity and communicates with other objects. The objects' owners should be able to police their communication so that objects do not accidentally disclose information about their owner. Transparency of ubiquitous computing, but also proliferation of biometric identification solutions are prerequisites for empowering users in choosing their personal privacy configurations. Biometric and surveillance technologies will affect first of all the conventional world outside the IMA, but may also influence the digital world. On one hand, the IMA could be safeguarded by biometrics. On the other hand, the IMA should mimic the knowledge others get by applying biometrics and surveillance technologies.

Assuming there will be the appropriate legislation in place, most players will be working to establish and keep trustworthiness. In Europe, this will be realised firstly by IT security and privacy evaluations together with a seal of quality and secondly by the Open Source approach and other transparency measures. Suppliers will have to convince their customers of their trustworthiness. Some people will prefer "buddy services", as "one of them" instead of organisations will help with identity management functionality.

Transparency facilitates trust. It may be the most important property of an IMS as regulation and other application-specific constraints could reduce the degrees of freedom of a user in deciding on the management of his or her partial identities. One could imagine that IMS in totalitarian states not only incorporate strict rules with almost no real possibility to decide on

---

<sup>227</sup> See Chapter 2.1.6.2.

---

one's data, but also contain backdoors. That kind of implementation of IMS would rather be privacy-enhancing as the existence of backdoors may lead to misuse of personal data.

Users will not accept (and have not, so far, accepted) IMA which they do not trust. After being more and more equipped with all kinds of technology and a de-facto standard of IMA use in professional lives, people could allow themselves the luxury or the carelessness to do without IMA whenever possible, e.g., in their spare time. So there might be different streams of people who always use IMA and others who like to abandon extra technology. At least in personal communication the wide-spread use of IMA is unlikely, but most people will profit from IMA help in communication with organisations.

The European legislator has already taken a first important step in the right direction with the Directives on electronic signatures and on data protection. The legal framework now has to be completed providing a good balance between individual rights and law enforcement, and between freedom of innovation and interoperability (and ability to be assessed) of the identity management technologies. Otherwise individual freedom and data protection in the open digital environment will not be able to thrive.

### 7.3 Summary

IMS is a topic for both today and the future. This Chapter has outlined roadmaps for the development of identity management technologies concentrating on different properties. The RAPID roadmap shows which research questions could be elaborated in the next few years, categorised in short-term (0-3 years), mid term (3-5 years) and long term (5-10 years). Especially client-side, server-side and infrastructure technologies are separately analysed. The demand for interdisciplinary research, integrating technological, legal and socio-economic aspects, is pointed out.

Another roadmap sketched in this Study shows the market penetration of key enabling and identity management-related technologies such as chipcards, biometrics, PDAs, broadband access, and ubiquitous computing, estimated until the year 2020: In the next few years progress especially in network access is to be expected. The market penetration of ubiquitous computing will at first slowly grow, but then may have a break-through in 2015. Additionally, the potential development of trusted computing technology is explained, whose market acceptance and penetration is however dependent on too many factors for a serious prognosis.

The roadmap on market penetration of IMS during the same period is structured into three scenarios: growth, steady-state and regression. Enabling and mitigating factors and constraints are analysed and described for all three scenarios. The key parameters will be usability, integration in other accepted applications, legal requirements, infrastructures, and technological maturity. Historical parallels to other technologies' market penetration can be drawn for digital signatures and PKI.

These three scenarios are varied when the maturity of concepts and applications is analysed. The existence of a gap between the concept and the application level is quite natural for all kind of new technologies or research. In the case of identity management the concepts seem to have emerged early without having seen any serious attempt to implement them for years: It was an idea ahead of its time. Only in the mid-90ies did the refinement of concepts and development of applications gain momentum.

The outlook then takes the optimistic prognosis of IMS development and describes what a world with users, who live with new technologies and are capable to use their IMA, could look like. Software agents, biometrics and PDAs could promote the user's self-determination, third parties could offer various services to help managing identities. Users would be educated, the legal framework would support anonymity and pseudonymity. The sketched picture shows a

subset of related areas of society which might change; in fact all parts will be affected by IMS in some way or another.



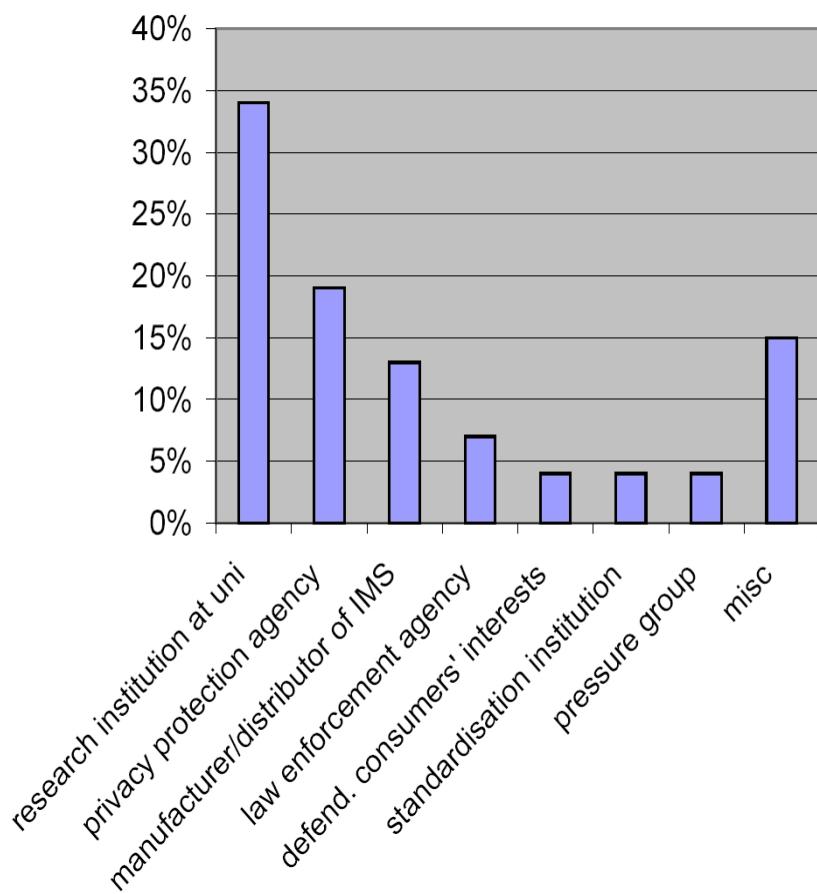
## 8 [CHAPTER H: QUESTIONNAIRE]

While elaborating this study, the authors conducted a survey on Identity Management Systems among a group of experts from economics, politics, science and privacy protection organisations. The primary aim of the survey was to find out and just describe experts' ideas of technology-based identity management. The chosen experts were sent a mainly standardised questionnaire by e-mail. This Chapter gives an overview of the results of the survey basing on the answers of the experts who filled in the questionnaire (further on called "responding experts"). Additional material regarding the questionnaire is provided in Annex 1.

### 8.1 Background of the Responding Experts

Who are the experts dealing with Identity Management Systems? First we were interested in the institutional and positional background of the experts who were sent the questionnaire.

#### Institutional Background

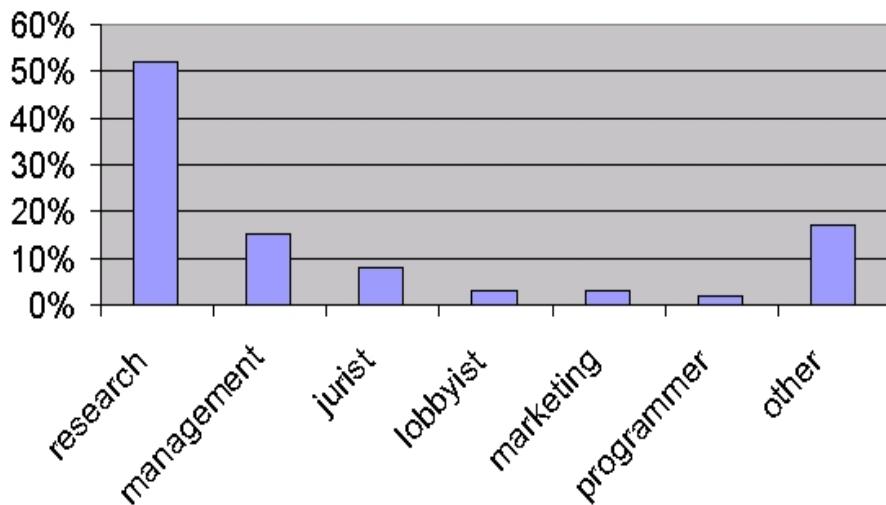


**Figure 93: Institutional Background of Responding Experts**

In addition, about 25 % of responding experts stated that they work for an institution other than those mentioned above. As we see from Figure 93, the most typical constellation was the employment in a research and management context. The question for the number of employees in the various institutions gave no appropriate hint on the question if merely single persons and small start-ups or rather established large institutions deal with the identity management subject. The figures lead to the assumption that there is some kind of balance.

---

## Position in Organisation



**Figure 94: Positions of Responding Experts in Their Organisation**

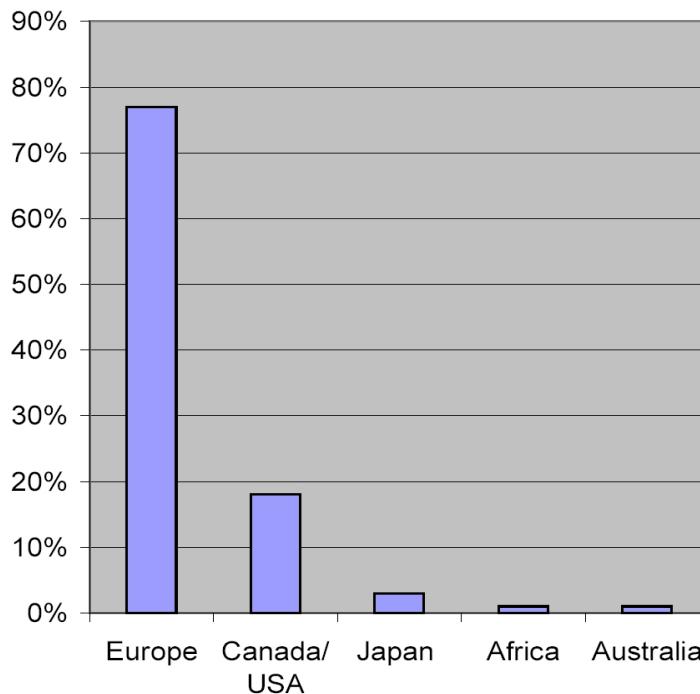
This unambiguously strong surplus of scientists (cf. Figure 94) had neither been planned nor had it been predictable. The aim was a socially neutral collection of e-mail addresses of the experts to be addressed. The list had been created by use of lists of conference participants, personal knowledge, results from search engine queries and contact addresses from web pages maintained by application manufacturers.<sup>228</sup> Even if it is to be considered that scientists are probably rather willing to answer questions for reasons of scientific solidarity than marketing experts and lawyers, these numbers point out that the identity management subject is still in a research and conception phase.

Next we took a closer look to the cultural background of the responding experts (cf. Figure 95):

---

<sup>228</sup> As far as the manufacturers' addresses are concerned, it was often only possible to send the questionnaire to a general e-mail address (such as, e.g., info@ddd.com). Experience has shown that specific reactions to a sophisticated query may not be expected.

## Cultural Background



**Figure 95: Cultural Background of Responding Experts**

Among the big block "Europe" Germany was the answer in 34 % of all cases, UK in 8 %, Netherlands 7 %. Overall German scientists form with 21 % the largest group among the responding experts.<sup>229</sup>

To investigate the interests of the asked experts, we used a predefined list of possible special interests concerning an Identity Management System. A hierarchical cluster analysis of these interests showed that the responding experts distinguish between two groups of aspects: On the one hand, there is the group of aspects with a rather technologic-operative orientation. This group includes the following aspects:

- *range of function,*
- *usability,*
- *privacy protection,*
- *security,*
- *access rights management* and
- *multiple application usage.*

The interest in *security* and *privacy protection* as well as *access rights management* and *multiple application usage* are statistically very closely related here.

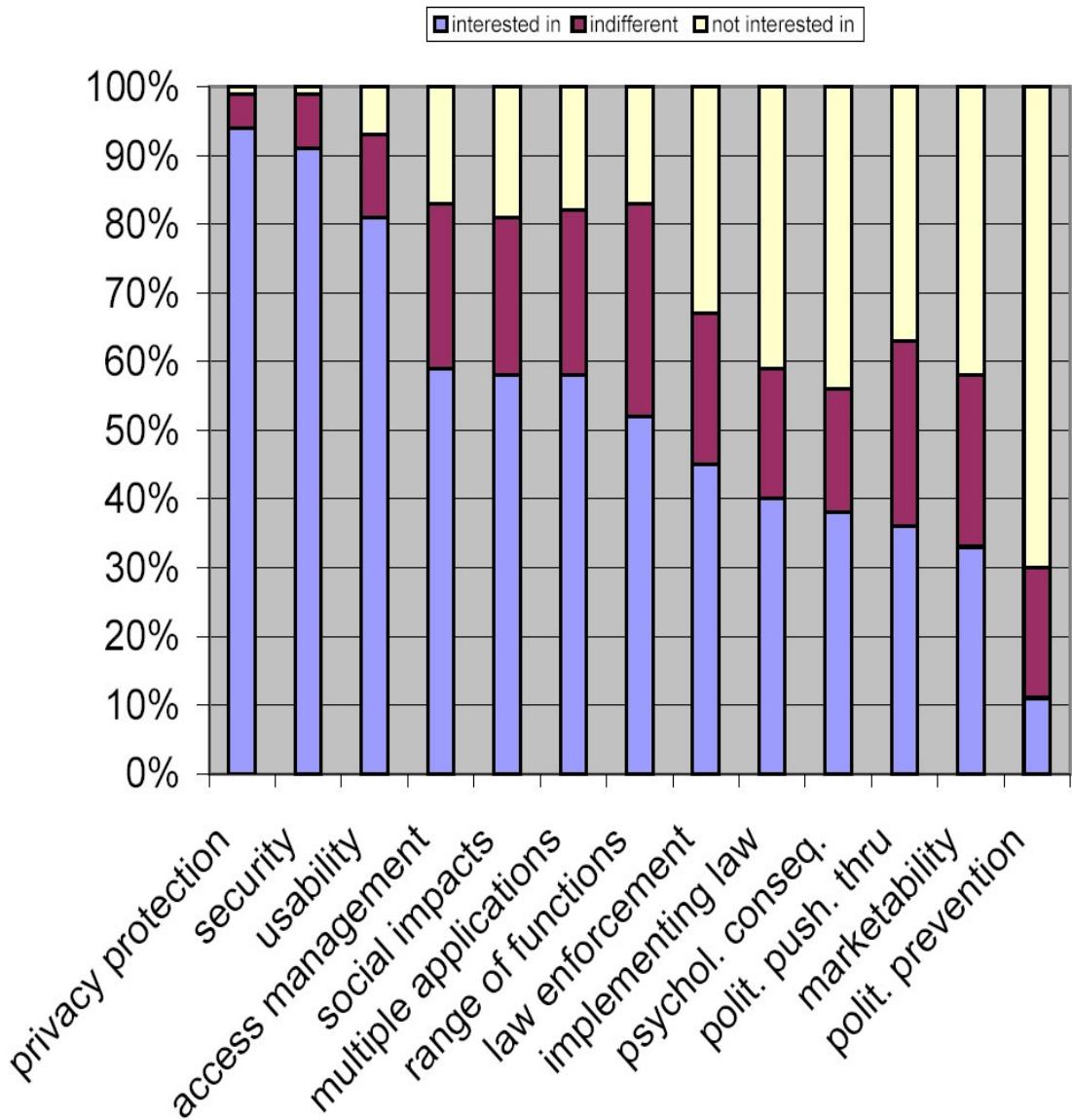
The second group of interests includes social aspects such as:

- *marketability,*
- *politically pushing through,*
- *implementing law,*
- *social impacts of implementation/use,*
- *psychological consequences* and
- *law enforcement.*

<sup>229</sup> Please note that the question for the cultural background is not to be regarded as equal to the countries in which the interviewees work and to the laws of which they are subject.

In this second group, too, there are two interest pairs of aspects that are particularly closely related: firstly *politically pushing through* and *implementing law*, secondly *social impacts* and *psychological consequences*. The answers to the question for an interest in a political prevention of an IMS could not be assigned to any of these two groups of orientation. The noticeable point of the result of this grouping is that, as far as identity management is concerned, privacy protection is primarily assigned more to a technological and less to a social context.

## Interests



**Figure 96: Interests of Responding Experts**

It is not surprising: The aspects that were most interesting to the responding experts are privacy protection followed by security (cf. Figure 96). Least interest was shown towards the psychological questions as well as the marketability and planned laws concerning IMS – in contrast to a definitely existing interest in the social effects of an IMS implementation or usage. Naturally, the employees of IMS manufacturers are most strongly interested in marketability; at the same time, this is the same group which claimed to be indifferent to this question. This would be a characteristic position for scientists who should be interested in the economy of their research but actually are not, in order to maintain their scientists' image. According to the

figures, 6 % are purely interested in IMS in terms of economy. This, too, is another hint at the circumstance that technology-based identity management needs more research and that society is not yet ready for it.

At last there are two other interesting statements which highlight the experts' know-how. Firstly, 19 % of the (assumed) experts who filled in the questionnaire had not dealt with the topic "Identity Management" until the time of the interview (April/May 2003), 21 % had dealt with this subject for only a few months. After all the majority of 34 % of the responding experts had been interested in the subject for two to four years. Still, 9 % stated that they had dealt with the subject for ten years or more. These experts work in the research and management area, one is a lawyer. Secondly, 28 % of the responding experts answered in the affirmative to the question if they use an Identity Management System<sup>230</sup>. These users are mainly employees of companies that manufacture Identity Management Applications. Within the large group of university scientists, only 20 % use an IMS. The following identity management products were mentioned: "*jap*", "*CookieCooker*", "*Netscape + Intranet based on INFORMIX*", "*Internally-developed solutions using Informix RDBMS*", "*Passport*", "*PGP, Windows PKI, .Net Passport*", "*smartcard*", "*FINEID, Teamware*", "*Self developed*", "*IBM Role Your Own*", "*Sun ONE Directory Server, migrating to Sun ONE Identity Server*", "*in-house*". Some other mentioned general communication applications they deploy in terms of Identity Management Applications: "*Kmail, Mutt, Konqueror, Opera*", "*Lotus products*", "*GSM SIM*", "*different browsers/e-mail agents*", "*PC*". This is yet another indicator for the diversity in interpretation of what an Identity Management System could be.

In the next Chapter we investigate the responding experts' ideas of technology-based identity management.

## 8.2 Estimations on Identity Management

In the sequel, we describe the main results of the survey with respect to applications, essential functions, possible marketability, bottlenecks regarding mass adoption, requirements for use within society, degree of centralisation in administration of personal data, possible socio-psychological consequences, and the effect on law enforcement.

### 8.2.1 Applications for Identity Management

As described in the previous paragraph, 28 % of all responding experts use an Identity Management System. When being asked which Identity Management System currently on the market they would call "state-of-the-art", 24 % of the responding experts answered with "*none*", another 24 % with "*Passport*", 47 % specified another product and 6 % stated they had no idea or experience.

The following Identity Management Applications have been mentioned whereas it seems as if mainly developers and marketing people did not try to objectively crown a leading product "state-of-the-art" but to call the application they deal with most. From these answers, it may be assumed that there is no program ruling the paradigm of an Identity Management Application without a doubt. Although "*Passport*" has been the mostly called application, about half of those who nominated it point out the weaknesses of Passport which disqualify it as state-of-the-art. Here we quote all the answers from the questionnaire:

- "*Network Identity of SUN Microsystems*"
- "*jap, the only one I ever used*"
- "*XMCARE from ICL/Simac for more information Mr Gilles van Blarkom +31703811308*"

---

<sup>230</sup> In the questionnaire the term "Identity Management System" was consistently used both in the meaning of a comprehensive IMS and in the meaning of the concrete Identity Management Application (see Chapter 1). Therefore the term IMS is used in this Chapter. The differentiation of IMS and IMA is a result of the research while elaborating this study.

- 
- "Pseudonyms provided by ISPs, anonymous proxies such as JAP, MIX networks such as Crowds"
  - "In-enterprise single signon and collaboration tools for employees. In-enterprise personalization tools for customers. Browser personalization. Microsoft Passport. Gator. Zero-knowledge. Roboform. Passlogix."
  - "TIVOLY – good, Oblix – interesting, CA eTrust – big market, PKI-services / products –not user friendly"
  - "Passport – they are still resolving legal and technical issues, I know of no adequate one."
  - "Anonymizer"
  - "I don't know of any good ones for protecting privacy that are fielded, but Stefan Brands 'private credentials' design is most advanced."
  - "The Parkinsonpas, a project in the Dutch City of Alphen a/d Rijn. By means of a chipcard combined with biometrics patients can personally decide to offer insight to their medical records to different medical agencies. Besides, the chipcard timely warns the patient to take his or her medicine"
  - "We have own solutions and we have used it some products; ID2, FINEID, and so on"
  - ".Net; Liberty Alliance; ZeroKnowledge; biometric technologies may be of assistance if used the right way – see OECD work here"
  - "Anonymisieren (AN.ON) P3P PGP, soweit Schutz gegen Dritte "
  - "Without privacy: Passport, Liberty Alliance, Addressing Privacy/self-determination: P3P implementations such as At&Ts Privacy Bird"
  - "Our implementation of IMS for a specific customer"
  - "Sun ONE Identity Server 6.0"
  - "Liberty Alliance is beginning to work."
  - "Netegrity Identity + Acces Management System"
  - "verisign – digital signature certification"

Note the diversity of ideas of which functionalities (.NET, Anonymizer, JAP, Privacy Bird, pseudonyms managed via ISPs, access management, digital signature verification ...) are already called Identity Management Systems in this context. It has to be assumed that the large part of those who did not answer this question simply had no actual application in mind. 9 % of those who answered could be called critics of the existing applications as they say explicitly they would not consider any of the present applications "state-of-the-art".

### 8.2.2      Essential Functions of an Identity Management System

A more theoretical perspective is provided by the question for the "essential functions of an IMS". This question was asked in an open manner, i.e., there were no predefined multiple choice answers offered. The given answers represent the diversity of ideas about the essential functions of an Identity Management System.

The general answers, often only consisting of single terms, nominated mostly "*privacy protection*" or "*security*" as essential functions of an IMS. There is one noticeable, outstanding generic answer: "*Linking the real world to the digital world without misusing identity*". This wording appears to the authors of this study as an felicitous and accurate generalisation of the essential function of an Identity Management System. This study basically develops a similar perspective by pointing out how much every aspect of social life is or will be affected by identity management. A second similarly generic answer, but rather focussed on political economy, is: "*Empower people and enable products*". And in one other case, the essential function of an IMS was seen in its "*ability to lie*".

Other more typical general answers about essential functions are e.g.: "*Ensure protection and privacy of personally identifiable information*" or "*It should help me to organise all my social relationships in a secure and privacy-protected form*" or "*Manage the virtual identities of the user. This should be done in a secure way, and protecting the privacy of the user.*" Or: "*Allowing a user to manage his or her own identities (plural meant), and to track and*

*understand how others are using those identities". Other answers are solely focussed on single aspects such as *anonymization, pseudonymity, trust, ease of use, range of functions* or somehow redundant on *identity protection*.*

It turns out that the overall answer focuses are diverse. For example, in a separate group of answers, identity management is called a management of roles: "*role management, user control of personal data, preferences management, user friendly interfaces, analysis and education*", "*correct, pervasive role changes on command and ease of use*", or "*Let the user choose different roles for different actions-prevent dissemination of personal data, if the user wants it – Manage certified data items, i.e., driving licence, digital ID card – (not really a function, but very important:) usability for inexperienced persons*", "*independent pseudonyms (identities) for different contacts or applications; automatic, transparent and reliable identification with suitable roles; easy control over information contained in a communicated pseudonym*".

A whole series of other statements argues differentiatedly and presents the experts' personal evaluations. "*Permitting the user to execute his right to informational self-determination; I am aware of the fact that this is a very high-level description – probably too high to be considered a function; my only excuse is that I have so far not seen anything that would merit being called an IMS.*" Or: "*Absence of single point of control. Possibility of multiple identity providers for each person, including the person itself. Privacy, meaning that all released data can be governed by policy, and a reasonable policy-management system, including user choices where not prescribed otherwise by existing regulations or contracts. Security. – Remark: I see marketability initially as a B2B case, and thus marketability as a question of what it initially offers to the participating enterprises. Hence I answer the next questions with respect to \*enterprises\* installing and paying for these systems, not end users as the authors may have meant.*" The following statement is particularly detailed and problem-oriented: "*user-controlled linkability; creation, use and choice of pseudonyms and related data sets (including certificates, attributes, credentials); context detection; configuration of rules to decide on roles/contexts and thus, (re-)use of pseudonyms; history function (transaction logging and interpretation); other support for the user to help him in privacy-enhancing management of his identities; privacy and security baseline (e.g., providing anonymity/unobservability in the communication network, crypto functionality for confidentiality and integrity (e.g., encryption, digital signatures incl. PKI), protection of the IMS itself against attacks); appropriate IMS infrastructure including specific IM-related services (e.g. identity brokers ...).*"

In another quite large group of answers, aspects oriented towards actual technology realisation are emphasised. Here, "*management of pseudonyms*" and "*user control of linkability*" (e.g., in: "*hide the linkage between my identity and my thoughts / interests / work*") is talked about. Furthermore, the following aspects are specified: "*automatic pseudonym switching according to context*", "*universal compatibility*", "*Providing multiple applications with personal data.*", "*integration with applications.*", "*(...) minimal data exchange & data trails where not.*", "*hiding personal data, negotiation of data disclosure, authentication, authorisation via credentials.*", "*identity editor, anonymity service*", "*Single Sign-On*", "*Caching decisions of the user once made in a certain context and remembering which information was left where.*", "*linking persons to identities in an unforgettable way, separating application domains, managing credentials*", "*Clear user interface; comprehensive approach to personal data, "Secure informational self-determination for data subjects"*", "*Avoid need for user to enter multiple passwords and usernames while maintaining a controllable level of anonymity and keeping use of pseudonyms under user control*", "*Support for Authentication, Authorisation, Auditability, Distributed Identity and Interoperability – preferably via open standards*".

There are only few answers that have a focus other than privacy, as shown by the following four statements on the essential functions of an IMS: "*Conveniently allows users to control distribution of information to vendors/web sites*" or: "*Proofs of Compliance to stated Policies*" or: "*facilitate online transactions*" or "*highly reliable identity authentication*". The small part of statements of this kind is noticeable because in popular computer magazines, identity management is often described in terms of those server processes that refer to the management

---

of access authorisation, granted privileges of digital users and their authentication by an organisation or across a series of organisations rather than in terms of user-controlled processes.

Overall, it can be derived from the answers that the majority of responding experts see the essential core function of an IMS in the protection of user's privacy by use of a secure, user-controlled technology. In this context, many statements point out that this could be realised via the user's control of the (un)linkability of different social roles supported by pseudonym management based on an anonymous communication infrastructure. The noticeably different forms of frequent unspecific answers show on the one hand the non-existence of a fixed paradigmatic core concerning the functionality to be performed by an IMS, i.e., more or less, something can be chosen at will. On the other hand, it leads to the assumption that a whole series of functionalities are indispensable for the functioning of an IMS.

### **8.2.3 Marketability of an Identity Management System**

Considering the obvious complexity of technology-based identity management on the one hand and the generally increasing discussion of this topic in popular magazines on the other, it is of course very interesting how experts estimate the marketability of an IMS in terms of "people are willing to pay for it". Therefore, the experts were asked to estimate the present situation and make a prognosis for the coming 10 years. The comparison of the two bars in Figure 97 shows: The topic is believed to be developable.

The responding experts assumed that a society-wide implementation of a multi-purpose IMS (question V30, cf. Annex 1) would take an average of 11.55 years (standard deviation: 8.7). Many interesting comments of the following kind were added by the responding experts:

- *"Not in the foreseeable future"*
- *"Forever, unless government will enforce it"*
- *"Few Years, translated to '4 years'."*
- *"I will not live to see a society-wide implementation, translated to: 40 years (2 generations)"*
- *I don't think market forces will bring it about; there's too much overhead for anyone other than fanatics to use. Won't happen on a large scale unless regulation requires it or Microsoft implements it."*
- *"less than 10 years for more than 50 %"*
- *"forever"*
- *"Maybe in 20 years but maybe never. Not in the short term and not until very serious privacy abuses (well beyond identity theft) are observed."*
- *"extremely unlikely, since proofs of compliance are hard"*
- *"I don't think society wide-multi-purpose IMS is likely or desirable. We don't have all-use ID cards."*
- *"I do not consider that an important goal."*
- *"Impossible to realize"*
- *"depends on several developments, don't know"*

## Marketability of IMS

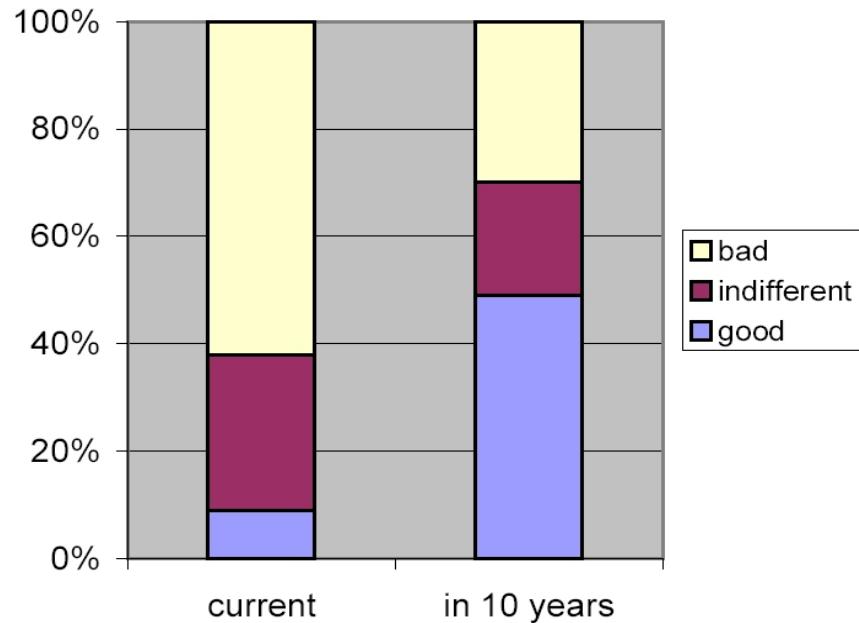


Figure 97: Marketability of IMS

### 8.2.4 Bottlenecks Regarding Mass Adoption of Identity Management Systems

The relatively most optimistic estimations were made by management experts; lawyers and scientists were most pessimist. As the main bottleneck for a successful society-wide implementation of an IMS, bad usability was assumed (60 %, cf. Table 33 – only one answer possible). Further on, too strong law enforcement which could prevent the social implementation is not considered the main bottleneck by most experts. The same is true for too weak law enforcement or the assumed costs caused by the implementation of IMS into society. Above all, the experts seem to be quite sure that possible problems of an IMS concerning the security and privacy will not play an outstanding role for the implementation.

Table 33: Potential Main Bottleneck Regarding Mass Adaption of IMS

	Frequency	Percent	Valid Percent	Cumulative Percent
Bad usability	48	53.9	60.0	60.0
Insufficient technological development	20	22.5	25.0	85.0
Insufficient security	7	7.9	8.8	93.8
Insufficient privacy protection	3	3.4	3.8	97.5
Too strong law enforcement	2	2.2	2.5	100.0
Too weak law enforcement	0	0.0	0.0	100.0
Too expensive	0	0.0	0.0	100.0
Total	80	89.9	100.0	
Missing	8	9	10.1	
Total	89	100.0		

---

Those experts who added comments mentioned mainly social aspects as potential bottlenecks. Four blocks of the responding experts' assumptions on the bottlenecks for implementing IMS can be distinguished:

1. User-oriented:

- "poor interest by the users"
- "If you think of user-side technology: insufficient market demand
- by end users to start introduction from that side (...)"

2. Society-oriented:

- "insufficient experience with computer/internet technology in the society"
- "insufficient knowledge for the need of it"
- "costs related to launching nation wide IMS"
- "Lack of standards"
- "too strong interests in non-privacy by government / intelligence / marketing industry"
- "(i) The risk of legislative initiatives which would negatively impact the mass deployment of IMS;  
(ii) (UK) Public antipathy towards anything which looks like an Identity Card ...  
(iii) Existing investment in closed/proprietary authentication systems"
- "Level of trust in both the technology and the institutions responsible for the use of the technology."
- "Priority of IMS in the corporate IT agenda"
- "Lesser incentives for those able to widely deploy and cause adoption."
- "lack of consensus about what IMS should be/look like; therefore slow adoption / slow standardisation"
- "**LACK OF AWARENESS FOR NEED AND ADVANTAGES IN CASE OF A USE AMONG THE SOCIETY**"

3. Technology-oriented:

- "insufficient pda / clients"
- "insufficient interoperability/scalability"
- "ineffectiveness due to location tracking and ubiquitous computing with biometric identification"
- "(...) lack of compatibility with enterprise single sign-on solutions."
- "bad interoperability"

4. Misc.:

- "Trust"
- "No reason would be the reason (i.e. the bottleneck is the fact that no one is sure about what is the bottleneck)."
- "When you are dealing with a DB of 10s-100s of millions of entries, you can't assume it's perfect. As long as proponents claim that it's perfect, there will be too many flaws and horror stories."

### **8.2.5      Important Aspects of an Identity Management System for Use on a Grand Scale within Society**

Another large series of questions deals with evaluating the importance of single aspects concerning the social usage of IMS. Here, a cluster analysis shows that there are four different groups:

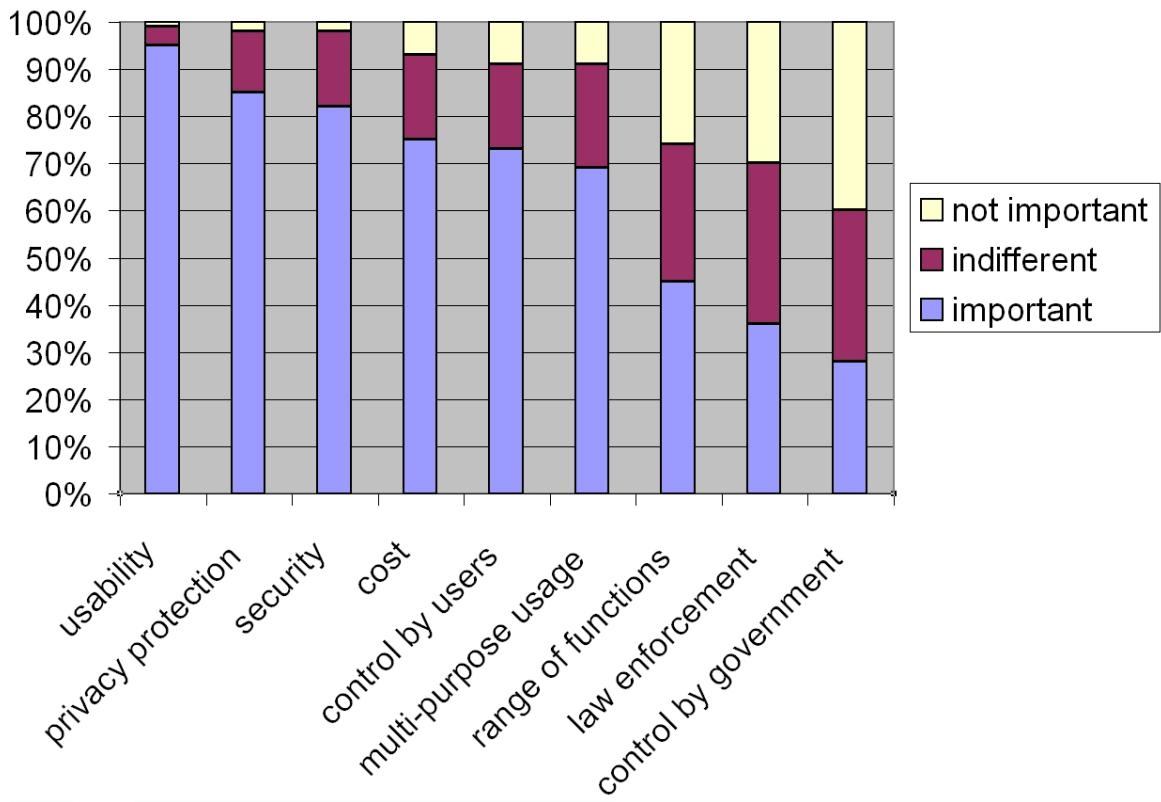
Group 1: "range of functions", "multi-purpose usage"

Group 2: "usability", "privacy protection", "security", "controllability for users"

Group 3: "cost"

Group 4: "controllability for government", "tracing of law enforcement resp. prosecution of claim"

## Important Aspects of an IMS



**Figure 98: Important Aspects of an IMS**

It could be assumed that good usability of a program genre is generally always important, but this evaluation probably reflects the suspicion that a technology-based identity management is so complex that the demands on usability are especially high – 95 % of the responding experts consider usability to be important (cf. Figure 98). 85 % of the responding experts regard privacy protection as important, followed by security (82 %). Here, indeed privacy protection and security are tightly related: it could actually be an IMS which turns out to be the highest privacy risk if it does not provide its functionality (including privacy-enhancing technology) on a secure level. In addition, an also important role is attached to the user's control by 73 %. 75 % assume that the costs caused by an IMS are important, 69 % consider multi-purpose usage to be important. The other aspects are estimated as rather unimportant: "range of functions" is for 45 % important, "tracing of law enforcement resp. prosecution of claim" for 36 %, and "controllability for government" is the only aspect that is assumed to be unimportant by the majority (40 %). The offered opportunity to name and evaluate another aspect has not been used by any of the responding experts.

### 8.2.6 Degree of Centralisation with Respect to the Administration of Personal Data

Regarding the question if the administration of personal data of an IMS should be carried out in a decentralised (by the user) or centralised way (by an organisation), 72 % of the responding experts were definitely in favour of the user's control of the personal data, but 24 % answered with a free statement instead. There were four different categories:

"Both should do ...":

- *"Both should do it. Users should be able to override what central administration does."*
- *"General information should be administered centrally with more sensitive data being administered by the user."*

- 
- "Technology should enable both. It's on the user to decide depending on the context he is in: Think of a world of mobile devices, where info has to be stored somewhere in the network."
  - "Both should be able"
  - "The relation between both alternatives above should be well balanced."
  - "A hybrid is probably optimal. Centralization of control is crucial to ensure good information, protect security, and even privacy of the data. That said, users need the power to ensure proper policies are enforced and retain control over how data is used, where possible."
  - "Administration should be federated, allowing the user to manage their own data even if it is held by a number of third parties with whom the user has some trust relationship."
  - "Decentralized, but users can only make changes that are screened."

"It depends on ...":

- "It depends on the data. For example, preferences should be decentralized; names and addresses should be centralized."
- "It depends on the different value of its parts, the costs of administration, and the advantage for the user."
- "Depending on the application."

"None of both, but ...":

- "By multiple independent third parties, which could be chosen by the user."
- "I think users will want numerous organizations to centralize parts of their identities, but not have any single organization knowing all about all of his or her various identities nor be responsible for all of the information his or her self."
- "Users would probably be willing to pay service providers to maintain their personal data."
- "government or banks"

Differentiations and discussions:

- "Under user control does not have to be client-side."
- "a) There should be a choice. It should be \*possible\* for user to do their own administration at least of data they choose themselves, and it should be made as easy as possible, but some people do prefer to have it done for them.  
b) There \*are\* data that only arise in interaction with organizations. For those the absence of single points of control is important, i.e., the data should remain in the individual organizations, and the system design should not require trust of these organizations in each other or in a central instance."
- "The priorities should be trust and security of data, followed by convenience and technical feasibility."
- "The users should decide on administration, so by default administration directly by the users themselves, but with the possibility to being supported by other parties."

### **8.2.7 Socio-Psychological Consequences of Usage of an IMS**

As already mentioned above, the responding experts seemed to be not very much interested in the psychological questions concerning identity management. Therefore, it is hardly astonishing that only 57 % expect psychological consequences from the usage of an IMS. These possible consequences were specified as follows:

More positive aspects mentioned:

- "stress levels and irritation at reduced functionality if use privacy enhancing technology"
- "Better confidence in person-to-person relations and in technology"
- "Distress from personal information being widely distributed. E.g. Clare Swire email about a year ago."
- "feeling of security and self responsibility by using the internet "

- "weariness and paranoia online should decrease slowly and slightly, as users are more in charge of who can see what they do and where they are. this is in my eyes the only reason why anybody should worry about identity management."
- "if the system is ok, so we have more trust"

More negative aspects mentioned:

- "No permanent, but it is easier to "kill people without looking in their eyes". Within the grey masses, people will be and act more radical."
- "Psychologically individuals want to control their lives, if not research show people will become depressed! (provided they are aware of it. It's a matter of consciousness)."
- "Depending on design: Feeling of loss of control. Feeling of more/less complexity in interactions. Feeling of trust/privacy."
- "There is psychological prerequisites for the usage of IMS, and as a consequence its use will have impact and consequences on the people who might use it. Awareness of surveillance but also maybe an increase sense of paranoia in others might occur."
- "The haunting feeling that somebody right now is selling your personal data, perhaps?"
- "People may not trust access management/credential-based decisions made by the IMS; people may be afraid of other parties sneakily accessing personal data."
- "1. Everything one does has psychological consequences :-)  
2. People will be more aware on who knows what about them on the net, at they will use this knowledge."
- "several: loss of control, identity, responsibility"
- "I think there are important issues of control and disempowerment."
- "there should be worries about personal data protection"
- "Users are going to have to trust the IMS system(s). This is a psychological notion; the less trust there is the less use there will be and the more fear and uncertainty will be produced"
- "Potentially, users will not trust the IMS with their data unless it is clear to them what protection it offers – logical, procedural and liability"
- "Possibly being out of order an human if IMS doesn't work"

Indifferent about positive or negative:

- "Complex question. It may be that people have very different propensities to divide their behaviour under different personae, or that latent propensities may emerge more widely than imagined. It may also be that greater awareness of privacy risks may not be matched by peoples ability to use protecting systems, leading to anxiety or resignation. It might stimulate emergence of interesting sub-cultures, and social engagement, but it might also have divisive tendencies. Needs lot of research, simulation and experiment."
- "the same as using ATMs, other (smart-)card-based systems, cellular phones etc."
- "creation of new sensitivities; creation of new senses of entitlement"
- "Big Brother" – no longer will internal moral systems be necessary because external surveillance could provide it all."

Concrete thesis, the "role explication" aspect:

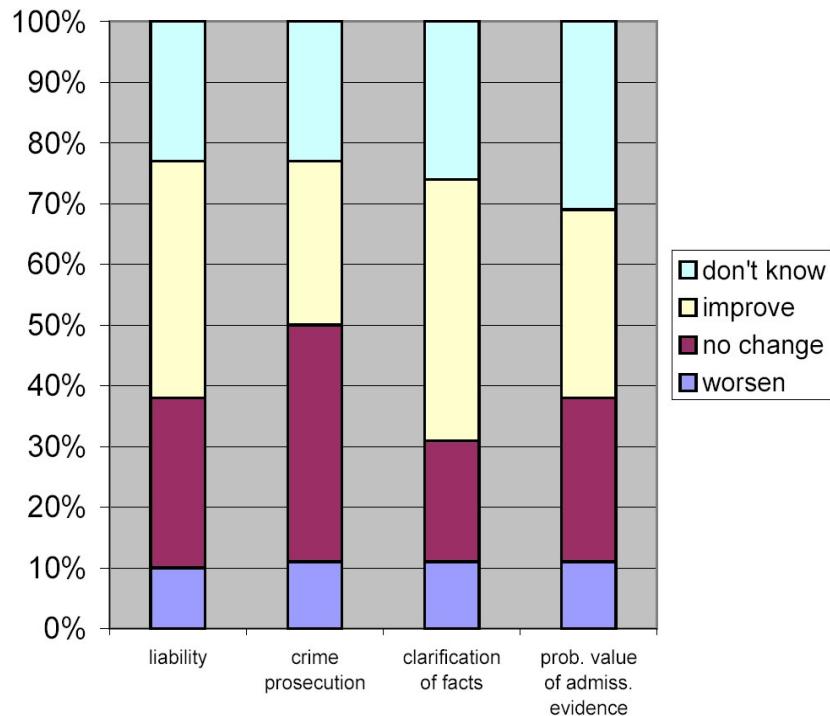
- "Explication of hidden or repressed aspects of life, personality, identity"
- "e.g. change in awareness about roles; growing dependency of IMS (and therefore problems when IMS is not properly available)"
- "people may become more aware of their various fragmented selves"
- "The stability persons identity is very important to them. Giving a person ease in presenting pseudonyms may blur his/her sense of identity and integrity."
- "People will develop higher awareness of the importance of their partial identities. Unfortunately, we have a chicken-and-egg-problem here: This is not only a likely consequence, but also a prerequisite for the adaptation of IMS."
- "You have to handle all your identities explicitly."

Although the answers can be categorised in content, nearly every answer in which a particular aspect is mentioned shows the complexity of this subject.

### 8.2.8 Estimated Effect on Law Enforcement

The last large catalogue of questions includes estimations concerning the effect of IMS on law enforcement, respectively prosecution of claim. Amazingly stable, 10 % to 11 % of the responding experts assume that IMS will cause deterioration concerning "crime prosecution", "clarification of facts", "probative value of admissible evidence" and "liability" as aspects, which play a specific role in law enforcement respectively prosecution of claim (cf. Figure 99). These apprehensions are predominantly located in the scientist group. 39 % believe that there will be no changes concerning crime prosecution. 43 % foresee that "clarification of facts" will improve by use of IMS. There is no coherent prognosis of the possible influence of Identity Management Systems in relation to law enforcement respectively prosecution of claim. From these results we may arrive at the following careful conclusion: There could be a chance for improving some aspects. Only a few of the responding experts think that the juridical situation become worse. But overall there is a high degree of uncertainty among the experts: A notably big part of them admits that they just "don't know".

**Effects of IMS on Law Enforcement  
resp. Prosecution of Claim**



**Figure 99: Effects of IMS on Law Enforcement Respectively Prosecution of Claim**

### 8.3 Summary

In the perception of most of the responding experts, Identity Management Systems are rather the subject of a predominantly technologically oriented research than already real products. However, a few of the responding experts understand a privacy-reflecting dealing with standard communication software as technology-based identity management. An extensively fixed paradigm of what makes and includes an IMS has obviously not gained general acceptance, yet.

The current marketability for specific IMS products is mainly estimated as being poor. The future marketability for the next 10 years, in contrast, is predicted to be good. However, many of the experts have their general doubts, assuming that the problems lie rather in the social

environment (insufficient standards, low user interest etc.) than in the area of the technological problems to be solved (privacy, security). The currently (at least claimed to be) most frequently deployed Identity Management Application is Microsoft's "Passport".

Above all, *privacy protection* and *security* have been named as essential functions of an IMS. In the more detailed answers, role management was emphasised. As particularly important for a society-wide usage of an IMS, usability was pointed out. In the practical realisation, IMS means to most of the responding experts an increasing comfort by "single sign-on" from the user's point of view. The technology-oriented experts consider the management of pseudonyms with the aim of avoiding linkability as the basic technology of identity management. The psychological consequences of the usage of an IMS are seen in the circumstance that all future communication, including the complete role design, will have to take place explicitly. On the one hand, this can improve the users' confidence in themselves and others, but on the other hand, the complexity of IMS can make the users unconfident and nervous. As far as the aspects of legal prosecution are concerned, uncertainty on future effects of IMS prevails. About 10 % of the experts assume that the situation will become worse while the majority predict an improvement caused by the use of IMS.

---

## REFERENCES

- [ANEC 2003] Consumer Requirements in Standardisation relating to the Information Society; ANEC – European Association for the Co-ordination of Consumer Representation in Standardisation; Version August 2003; <http://www.anec.org/attachments/it008-03rev.pdf>.
- [Art. 29 DPWP 2003] Article 29 Data Protection Working Party: Working Document on on-line authentication services; WP 68; 10054/03/EN; adopted on 29 January 2003; [http://europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2003/wp68\\_en.pdf](http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_en.pdf).
- [Baecker 1999] Dirk Baecker: Organisation als System; Suhrkamp, Frankfurt am Main 1999.
- [Bahlow 1985] Hans Bahlow: Deutsches Namenlexikon; 1<sup>st</sup> edition; Suhrkamp, Frankfurt am Main 1985.
- [Bäumler/von Mutius 2003] Helmut Bäumler, Albert von Mutius (Eds.): Das Recht auf Anonymität; Vieweg, Wiesbaden 2003.
- [Berman/Bruckman 2001] Joshua Berman, Amy S. Bruckman: The Turing Game – Exploring Identity in an Online Environment; in: Convergence, 7 (3), 83-102, 2001; <http://www.cc.gatech.edu/fac/Amy.Bruckman/papers/convergence-tg-01.pdf>.
- [Beck 1986] Ulrich Beck: Risikogesellschaft – Auf dem Weg in eine andere Moderne; Suhrkamp, Frankfurt am Main 1986.
- [Berthold/Federrath/Köhntopp 2000] Oliver Berthold, Hannes Federrath, Marit Köhntopp: Project "Anonymity and Unobservability in the Internet"; Workshop on Freedom and Privacy by Design; in: Proceedings of the Tenth Conference on Computers, Freedom & Privacy, CFP 2000: Challenging the Assumptions, Toronto/Canada, April 4-7, 2000; ACM, New York 2000; 57-65.
- [Berthold/Köhntopp 2001] Oliver Berthold, Marit Köhntopp: Identity Management Based On P3P; in: Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies; Proc. Workshop on Design Issues in Anonymity and Unobservability; LNCS 2009; 2001; 141-160.
- [Beslay/Punie 2002] Laurent Beslay, Yves Punie: The Virtual Residence: Identity, Privacy and Security; in: IPTS Report 67; JRC Seville, September 2002; 17-23; <http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html>.
- [Bianchi 1963] Cesa Bianchi in: Enciclopedia della Scienza e della Tecnica, Vol. VII, item: Personalità (Personality)], Milan 1963; 781.
- [Birch 2002] David G.W. Birch: Now we can be open – A white paper on doing business in a world of open networks; <http://www.hyperion.co.uk/PubWebFiles/openforbusiness.pdf>.
- [Bogdanowicz/Beslay 2001] Marc Bogdanowicz, Laurent Beslay: Cyber-Security and the Future of Identity; in: IPTS Report No. 57; JRC Seville, September 2001; 28-35; <http://www.jrc.es/pages/iptsreport/vol57/english/ICT4E576.htm>.
- [Borking/Raab 2001] John J. Borking, Charles D. Raab: Laws, PETs and other Technologies for Privacy Protection; Refereed Article; Journal of Information, Law & Technology (JILT), Issue 1, 2001; <http://elj.warwick.ac.uk/jilt/01-1/borking.html>.
- [Brands 1999] Stefan Brands: Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy; Thesis; Brands Technologies; 1999.

- [Camenisch/Lysyanskaya 2001] Jan Camenisch, Anna Lysyanskaya: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation; in: Birgit Pfitzmann (Ed.): Advances in Cryptology – EUROCRYPT 2001, LNCS 2045; Springer, Berlin 2001; 93-118.
- [Chaum 1981] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; in: Communications of the ACM, Vol. 24 No. 2, February 1981; 84-88.
- [Chaum 1984] David Chaum: A New Paradigm for Individuals in the Information Age; in: Proc. of the 1984 Symposium on Security and Privacy; IEEE, Oakland 1984; 99-103.
- [Chaum 1985] David Chaum: Security Without Identification: Transaction Systems to Make Big Brother Obsolete; in: Communications of the ACM, Vol. 28 No. 10, October 1985; 1030-1044; [http://www.chaum.com/articles/Security\\_Wthout\\_Identification.htm](http://www.chaum.com/articles/Security_Wthout_Identification.htm).
- [Chaum/Evertse 1987] David Chaum, Jan-Hendrik Evertse: A secure and privacy-protecting protocol for transmitting personal information between organisations; in: M. Odlyzko (Ed.): Advances in Cryptology – CRYPTO '86, LNCS 263; Springer, Berlin 1987; 118-167.
- [Chaum 1990] David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt '90, LNCS 453, Springer, Berlin 1990, 246-264.
- [Chen 1995] Lidong Chen: Access with pseudonyms; in: E. Dawson, J. Golic (Eds.): Cryptography: Policy and Algorithms, LNCS 1029; Springer, Berlin 1995; 232-243.
- [Clarke 1993] Roger Clarke: Computer Matching and Digital Identity; in: Proceedings of the Computers, Freedom & Privacy Conference; San Francisco 1993; <http://www.anu.edu.au/people/Roger.Clarke/DV/CFP93.html>.
- [Clarke 1999] Roger Clarke: Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice; in: S. Fischer-Hübner, G. Quirchmayr, L. Yngström (Eds.): User Identification & Privacy Protection: Applications in Public Administration & Electronic Commerce; Kista, Schweden, June 1999; IFIP WG 8.5 and WS 9.6; <http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html>.
- [Clauß/Köhntopp 2001] Sebastian Clauß, Marit Köhntopp: Identity Management and Its Support of Multilateral Security; in: Computer Networks 37 (2001); Special Issue on Electronic Business Systems; Elsevier, North-Holland 2001; 205-219.
- [Clauß/Pfitzmann/Hansen/Van Herreweghen 2002] Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, Els Van Herreweghen: Privacy-Enhancing Identity Management; in: IPTS Report 67; JRC Seville, September 2002; 8-16; <http://www.jrc.es/pages/iptsreport/vol67/english/IPT2E676.html>.
- [Cranor 1999] Lorrie Faith Cranor: Agents of Choice: Tools that Facilitate Notice and Choice about Web Site Data Practices; in: Proceedings of the 21st International Conference on Privacy and Personal Data Protection, 13-15 September 1999, Hong Kong SAR, China; 19-25.
- [Cranor/Resnick 2000] Lorrie Faith Cranor, Paul Resnick: Protocols for Automated Negotiations with Buyer Anonymity and Seller Reputations; NetNomics 2000; Vol. 2, Issue 1; 1-24.
- [Damgaard 1990] Ivan Bjerre Damgaard: Payment systems and credential mechanism with provable security against abuse by individuals; in: Shafi Goldwasser (Ed.): Advances in Cryptology – CRYPTO '88, LNCS 40, 328-335; Springer, Berlin 1990.

---

[Damker/Pordesch/Reichenbach 1999] Herbert Damker, Ulrich Pordesch, Martin Reichenbach: Personal Reachability and Security Management – Negotiation of Multilateral Security; in Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications. Vol. 3, Addison-Wesley, München 1999; 95-111.

[Döring 1999] Nicola Döring: Sozialpsychologie des Internet – Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen; Hogrefe, Göttingen 1999.

[Dumortier 2002] Jos Dumortier, Caroline Goemans: Roadmap for European Legal Research in Privacy and Identity Management; <http://www.ra-pid.org>.

[Dyson 2002a] Esther Dyson: Release 1.0, Volume 20, No. 6/7, 28. June 2002/25. July 2002 – Digital Identity Management/Personal Identity Management: The Applications.

[Dyson 2002b] Esther Dyson: Digital Identity in Context; in: IPTS Report 67; JRC Seville, September 2002; 4-7; <http://www.jrc.es/pages/iptsreport/vol67/english/IPT1E676.html>.

[Egger/Abrazhevich 2001] Florian N. Egger, Dennis Abrazhevich: Security & Trust: Taking Care of the Human Factor; Electronic Payment Systems Observatory Newsletter, Vol. 9; JRC Seville 2001; <http://epso.jrc.es/newsletter/vol09/6.html>.

[Endruweit/Trommsdorf 1989] Günter Endruweit, Gisela Trommsdorf (Eds.): Wörterbuch der Soziologie; 3 Vol.; Enke, Stuttgart 1989.

[Enzmann/Schulze 2001] Matthias Enzmann, Günter Schulze: DASIT: Privacy Protection in the Internet by User Control; Electronic Payment Systems Observatory (ePSO) Newsletter Vol. 9, September 2001; <http://epso.jrc.es/newsletter/vol09/4.html>.

[Federrath 1999a] Hannes Federrath: Protection in Mobile Communications; in: Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications, Vol. 3: Technology, Infrastructure, Economy; Addison-Wesley, München 1999; 349-364.

[Federrath 1999b] Hannes Federrath: Sicherheit mobiler Kommunikation; DuD-Fachbeiträge; Vieweg, Wiesbaden 1999.

[Ferrara 1941] Ferrara: Diritto delle persone e di famiglia, Naples 1941; 85.

[FIPS 1977] U.S. Department of Commerce, National Bureau of Standards: FIPS PUB 48 – Guidelines on Evaluation of Techniques for Automated Personal Identification; Washington, D.C., USA, April 1, 1977.

[Fischer-Dieskau/Gitter/Paul/Steidle 2002] Stephanie Fischer-Dieskau, Rotraud Gitter, Sandra Paul, Roland Steidle: Elektronisch signierte Dokumente als Beweismittel im Zivilprozess; in: Multimedia und Recht (MMR); Verlag C.H. Beck, München 2002; 709.

[Fischer-Hübner/Nilsson/Lindskog 2002] Simone Fischer-Hübner, Mikael Nilsson, Helena Lindskog: Self-Determination in the Mobile Internet; IFIP SEC 2002 Conference Proceedings; May 2002, Kluwer.

[von Foerster 1985] Heinz von Foerster: Sicht und Einsicht – Versuche zu einer operativen Erkenntnistheorie; Carl Auer Systeme Verlag, Wiesbaden, Braunschweig 1985.

[Frey/Irle 1985] Dieter Frey, Martin Irle (Eds.): Theorien der Sozialpsychologie; Vol. 2: Gruppen und Lerntheorie; Huber, Bern 1985.

- [Freud 1978] Siegmund Freud: Das Ich und das Es und andere metapsychologische Schriften; Fischer, Frankfurt am Main 1978.
- [Friedman/Resnick 2001] Eric Friedman, Paul Resnick: The Social Cost of Cheap Pseudonyms; Journal of Economics and Management Strategy 10(2); 2001; 173-199; earlier version presented at the Telecommunications Policy Research Conference, Washington, DC, October 1998.
- [Fuchs et al. 1978] Werner Fuchs et al. (Eds.): Lexikon zur Soziologie; 2<sup>nd</sup> edition; Westdeutscher Verlag, Opladen 1978.
- [Gehlen 1956] Arnold Gehlen: Urmensch und Spätkultur; Athenäum, Bonn 1956.
- [Gerck 1998] Ed Gerck: Toward Real-World Models of Trust: Reliance on Received Information; Work document; first published on Jan 23rd, 1998 in the mcg-talk list server; <http://www.mcg.org.br>.
- [Gerhardt 1971] Uta Gerhardt: Rollenanalyse als kritische Soziologie; 1<sup>st</sup> edition; Luchterhand, Neuwied/Berlin 1971.
- [Giddens 1991] Anthony Giddens: Modernity and Self-Identity: Self and Society in the Late Modern Age; Polity Press, Cambridge 1991.
- [Goffman 1986] Erving Goffman: Interaktionsrituale – Über Verhalten indirekter Kommunikation; 1<sup>st</sup> edition; Suhrkamp, Frankfurt am Main 1986 (published in 1967 for the first time).
- [Grandison/Sloman 2000] Tyrone Grandison, Morris Sloman: A Survey on Trust in Internet Applications; IEEE Communications Surveys & Tutorials, 4th Quarter 2000 issue; 2000.
- [Grimm/Roßnagel 2000] Rüdiger Grimm, Alexander Roßnagel: Datenschutz für das Internet in den USA; in: Datenschutz und Datensicherheit (DuD) 24/8 (2000); Vieweg, Wiesbaden 2000; 446-453.
- [Gundermann 2003a] Lukas Gundermann: Anonymität, Pseudonymität und E-Government – geht das?; in: Helmut Bäumler/Albert von Mutius (Hrsg.): Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts; Vieweg, Wiesbaden 2003: 117-137.
- [Gundermann 2003b] Lukas Gundermann: Sozialhilfe für Dagobert Duck – Sind Anonymität und Pseudonymität im E-Government möglich? in: Datenschutz und Datensicherheit (DuD), 27/5 (2003); Vieweg, Wiesbaden 2003: 282-286.
- [Habermas 1985] Jürgen Habermas: Theorie des kommunikativen Handelns; Vol. 1 and 2; 3<sup>rd</sup> edition; Suhrkamp, Frankfurt am Main 1985 (published in 1981 for the first time).
- [Hagel/Singer 1999] John Hagel, Marc Singer: Net Worth – Shaping Markets When Customers Make the Rules; Harvard Business School Press, Boston 1999.
- [Hansen 2003] Marit Hansen: Privacy-Enhancing Technologies; in: Alexander Roßnagel (Ed.): Handbuch Datenschutzrecht; Verlag C.H. Beck, München 2003; 291-324.
- [Hansen/Berlich 2003] Marit Hansen, Peter Berlich: Identity Management Systems: Gateway and Guardian for Virtual Residences; accepted submission to EMTEL Conference 23-26 April, 2003; London; [http://www.lse.ac.uk/collections/EMTEL/Conference/papers/hansen\\_berlich.pdf](http://www.lse.ac.uk/collections/EMTEL/Conference/papers/hansen_berlich.pdf).

---

[Hansen/Köhntopp/Pfitzmann 2002] Marit Hansen, Kristian Köhntopp, Andreas Pfitzmann: The Open Source approach – opportunities and limitations with respect to security and privacy; in: Computers & Security Vol. 21 No. 5; Elsevier, North-Holland 2002; 461-471.

[Hansen et al. 2003] Marit Hansen, Henry Krasemann, Martin Rost, Riccardo Genghini: Datenschutzaspekte von Identitätsmanagementsystemen – Recht und Praxis in Europa; in: Datenschutz und Datensicherheit (DuD), 27/9 (2003); Vieweg, Wiesbaden 2003; 551-555.

[Hansen/Probst 2002] Marit Hansen, Thomas Probst: Datenschutzgütesiegel aus technischer Sicht: Bewertungskriterien des schleswig-holsteinischen Datenschutzgütesiegels; in: Helmut Bäumler, Albert von Mutius (Eds.): Datenschutz als Wettbewerbsvorteil – Privacy sells: Mit modernen Datenschutzkomponenten Erfolg beim Kunden; Vieweg, Wiesbaden 2002; 163-179; further information at <http://www.datenschutzzentrum.de/>.

[Hansen/Rost 2002] Marit Hansen, Martin Rost: Datenschutz durch computergestütztes Identitätsmanagement; in: Kubicek, Klumpp, Bülesbach, Fuchs, Roßnagel (Eds.): Innovation@Infrastruktur – Informations- und Dienstleistungsstrukturen der Zukunft; Jahrbuch Telekommunikation und Gesellschaft 2002, Vol. 10; Hüthig, Heidelberg 2002; 255-268; [http://www.netzservice.de/Home/maro/mr\\_dsidman.html](http://www.netzservice.de/Home/maro/mr_dsidman.html).

[Hansen/Rost 2003] Marit Hansen, Martin Rost: Nutzerkontrollierte Verkettung – Pseudonyme, Credentials, Protokolle für Identitätsmanagement; in: Datenschutz und Datensicherheit (DuD), 27/5 (2003); Vieweg, Wiesbaden 2003; 293-296.

[Hes/Hooghiemstra/Borking 1999] R. Hes, T.F.M. Hooghiemstra, J.J. Borking: At face value. On biometrical identification and privacy; Registratiekamer, September 1999; Achtergrondstudies en Verkenningen 15; [http://www.cbpweb.nl/downloads\\_av/AV15.pdf](http://www.cbpweb.nl/downloads_av/AV15.pdf).

[Hoffmann 1997] Ute Hoffmann: Die erträgliche Leichtigkeit des Seins – Subjektivität und Sozialität in der Netzwerk; in: G. G. Voß/H. J. Pongratz (Eds.): Subjektorientierte Soziologie – Karl Martin Bolte zum 70. Geburtstag; Leske + Budrich, Leverkusen 1997; 95-125.

[Huizenga 2003] Jan Huizenga: RAPID – Overall Roadmap; to be published 10. Sep. 2003; [http://www.ra-pid.org/default/page.gx?\\_app.page=entity.html&\\_app.action=entity&\\_entity.object=KM-----000000000000409&\\_entity.name=Overall-Roadmap](http://www.ra-pid.org/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM-----000000000000409&_entity.name=Overall-Roadmap).

[IEEE 1990] Institute of Electrical and Electronics Engineers: IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries; New York, NY, 1990.

[ISO9241 1996] ISO 9241-10: Ergonomic requirements for office work with visual display terminals (VDTs) – Part 10: Dialogue principles; 1996; <http://www.iso.org>.

[ISO12119 1994] ISO/IEC 12119: Information technology – Software packages – Quality requirements and testing; 1994; <http://www.iso.org>.

[ISO15408 1999] ISO/IEC 15408: Common Criteria; 1999; <http://csrc.nist.gov/cc/>.

[IWGDPT 2000] International Working Group on Data Protection in Telecommunications: Common Position on Infomediaries; 4-5 May 2000, Rethymno; <http://www.datenschutz-berlin.de/doc/int/iwgdppt/>.

[James 1890] William James: The Principles of Psychology, 1890 ("Classics in the History of Psychology"; <http://psychclassics.yorku.ca/>).

[Jendricke/Gerd tom Markotten 2000] Uwe Jendricke, Daniela Gerd tom Markotten: Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet; in:

Proc. 16th Annual Computer Security Applications Conference (ACSAC 2000), New Orleans, USA, December 11-15, 2000; <http://www.acsac.org/2000/papers/90.pdf>.

[Jendricke/Gerd tom Markotten 2001] Uwe Jendricke, Daniela Gerd tom Markotten: Identitätsmanagement: Einheiten und Systemarchitektur; in: Dirk Fox, Marit Köhntopp, Andreas Pfitzmann (Eds.), Verlässliche IT-Systeme – Sicherheit in komplexen Infrastrukturen; Vieweg, Wiesbaden 2001; 77-85.

[Jendricke/Kreutzer/Zugenmaier 2002] Uwe Jendricke, Michael Kreutzer, Alf Zugenmaier: Mobile Identity Management; Technical Report 178, Institut für Informatik, Universität Freiburg, October 2002; Workshop on Security in Ubiquitous Computing, UBICOMP 2002; <ftp://ftp.informatik.uni-freiburg.de/documents/reports/report178/report00178.ps.gz>.

[Jendricke 2002] Uwe Jendricke: Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement; Dissertation; Albert-Ludwigs-Universität Freiburg i.Br., Wirtschafts- und Verhaltenswissenschaftliche Fakultät; December 2002.

[Kelsen 1966] Quoted from Pizzorusso, Scialoja, Branca – page 3. Galgano, Struttura logica e contenuto normativo del concetto di persona giuridica, Riv. Dir. Civ., I, 553-633. Kelsen, La dottrina pura del diritto, Einaudi, 1966, 200; Teoria generale del diritto e dello stato, Etas, 1978; 101.

[Kent/Millett 2003] Stephen T. Kent, Lynette I. Millett (Eds.): Who Goes There?: Authentication Through the Lens of Privacy; Committee on Authentication Technologies and Their Privacy Implications, National Research Council; The National Academies Press, Washington, DC, 2003; <http://www.nap.edu/catalog/10656.html>.

[Kieserling 1997] Andre Kieserling: Kommunikation unter Anwesenden – Studien über Interaktionssysteme; Dissertationsschrift an der Fakultät für Soziologie der Universität Bielefeld, 1997.

[Kiss 1990] Gabor Kiss: Grundzüge und Entwicklung der Luhmannschen Systemtheorie, 2<sup>nd</sup> edition; Enke, Stuttgart 1990.

[Kneer/Nassehi 1993] Georg Kneer, Armin Nassehi: Niklas Luhmanns Theorie sozialer Systeme: Eine Einführung; UTB, München 1993.

[Koch/Wörndl 2001] Michael Koch, Wolfgang Wörndl: Community Support and Identity Management; in: Proc. Europ. Conference on Computer-Supported Cooperative Work (ECSCW2001); Bonn 2001; 319-338.

[Koch 2002] Michael Koch: Global Identity Management to Boost Personalization; in: P. Schubert, U. Leimstoll (Eds.): Proc. Research Symposium on Emerging Electronic Markets; Institute for Business Economics (IAB), University of Applied Sciences Basel; Basel 2002; 137-147.

[Köhntopp 1999] Marit Köhntopp: Identitätsmanagement – Anforderungen aus Nutzersicht; Talk at Workshop "Datenschutz und Anonymität" of NRW-Forschungsverbundes Datensicherheit, 22. November 1999 in Essen; in: Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen (Ed.): Datenschutz und Anonymität; Düsseldorf 2000; 43-55.

[Köhntopp 2000] Marit Köhntopp: Identitätsmanagement; Version: 2000-12-29; in: Helmut Bäumler, Astrid Breinlinger, Hans-Hermann Schrader (Eds.): Datenschutz von A-Z; Luchterhand, Neuwied 1999, 2000; [http://www.marithansen.de/pub/idmanage/def/Koehn\\_00dIdmanageDef.pdf](http://www.marithansen.de/pub/idmanage/def/Koehn_00dIdmanageDef.pdf).

---

[Köhntopp/Köhntopp 2000] Marit Köhntopp, Kristian Köhntopp: Datenspuren im Internet; in: Computer und Recht (CR) 16/4 (2000); Verlag Dr. Otto Schmidt, Köln 2000; 248-257.

[Köhntopp 2001] Marit Köhntopp: "Wie war noch gleich Ihr Name?" – Schritte zu einem umfassenden Identitätsmanagement; in: Dirk Fox, Marit Köhntopp, Andreas Pfitzmann (Eds.): Verlässliche IT-Systeme – Sicherheit in komplexen Infrastrukturen; Vieweg, Wiesbaden 2001; 55-75.

[Köhntopp/Pfitzmann 2001] Marit Köhntopp, Andreas Pfitzmann: Informationelle Selbstbestimmung durch Identitätsmanagement; in: it+ti Informationstechnik und Technische Informatik, Schwerpunktthema "IT-Sicherheit" 5/2001; Oldenbourg Wissenschaftsverlag, München, September 2001; 227-235.

[Kormann/Rubin 2000] David P. Kormann, Aviel D. Rubin: Risks of the Passport Single Signon Protocol; Computer Networks; Elsevier Science Press, vol. 33, 2000; 51-58; <http://avirubin.com/passport.htm>.

[Kreps/Wilson 1982] David M. Kreps, Robert Wilson: Reputation and Imperfect Information; Journal of Economic Theory; Vol. 27, Issue 2; 1982; 253-279.

[Kriegelstein 2002] Thomas Kriegelstein: Entwurf und Implementierung eines Identitätsmanagements anhand eines Beispielszenarios; Diploma Thesis; Dresden University of Technology, Faculty Informatics; February 2002.

[LA 2003a] Liberty Alliance Project – Liberty ID-FF Architecture Overview Draft Version 1.2-03; 14 April 2003; <http://www.projectliberty.org/>.

[LA 2003b] Liberty Alliance Project – Security & Privacy Implementation Guidelines Version 1.0-05; 14 April 2003; <http://www.projectliberty.org/>.

[Lacoste/Pfitzmann/Steiner/Waidner 2000] Gérard Lacoste, Birgit Pfitzmann, Michael Steiner, Michael Waidner (Eds.): SEMPER – Secure Electronic Marketplace for Europe; Lecture Notes in Computer Science Vol.. 1854; Springer, Heidelberg 2000.

[Lehnhardt 1995] Matthias Lehnhardt: Identität im Netz: das Reden von der "Multiplen Persönlichkeit"; in: Martin Rost (Ed.): Die Netzrevolution – Auf dem Weg in die Weltgesellschaft; Eichborn, Frankfurt am Main 1995; 108-123.

[Lessig 1999] Lawrence Lessig: Code and Other Laws of Cyberspace; Basic Books, New York, NY, 1999.

[LIBE 2003] LIBE Study: Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview; Report to the European Parliament prepared by IPTS, JRC Seville; Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE); Final Draft July 2003.

[Luhmann 1987] Niklas Luhmann: Soziale Systeme – Grundriß einer allgemeinen Theorie; 1<sup>st</sup> edition; Suhrkamp, Frankfurt am Main 1987 (published in 1984 for the first time).

[Luhmann 1989] Niklas Luhmann: Vertrauen – ein Mechanismus zur Reduktion von Komplexität; 3<sup>rd</sup> edition; Enke, Stuttgart 1989 (published in 1968 for the first time as No. 28 of "Soziologische Gegenwartsfragen").

[Luhmann 1991] Niklas Luhmann: Die Form 'Person'; in: Soziale Welt; 42. Jg., Heft 2, 1991; 167-175.

[Luhmann 1997] Niklas Luhmann: Die Gesellschaft der Gesellschaft; 1<sup>st</sup> edition; Suhrkamp, Frankfurt am Main 1997.

[Luhmann 2000] Niklas Luhmann: Organisation und Entscheidung; 1<sup>st</sup> edition; Westdeutscher Verlag, Opladen/Wiesbaden 2000.

[Lysyanskaya/Rivest/Sahai/Wolf 1999] Anna Lysyanskaya, Ron Rivest, Amit Sahai, Stefan Wolf: Pseudonym systems; in: Howard Heys, Carlisle Adams (Eds.): Selected Areas in Cryptography, LNCS 1758; Springer, Berlin 1999.

[Manfredini 2001] Arrigo D. Manfredini: Istituzioni di diritto romano, Giappichelli 2001; 75-96.

[Maturana 1982] Humberto Maturana: Erkennen – Die Organisation und Verkörperung von Wirklichkeit – Ausgewählte Arbeiten zur biologischen Epistemologie; Vieweg, Braunschweig/Wiesbaden 1982.

[Mead 1934] George H. Mead: Mind, Self and Society; Chicago Press 1934.

[MS 2000] Microsoft .NET Passport Press Room; Response to Kormann & Rubin, 2000.

[MS 2002] Microsoft .NET Passport Review Guide; The Why, What and How of Microsoft .NET Passport; March 2002.

[Nabeth/Roda 2002] Thierry Nabeth, Claudia Roda: Intelligent Agents and the Future of Identity; in: IPTS Report 67; JRC Seville, September 2002; 24-28; <http://www.jrc.es/pages/iptsreport/vol67/english/IPT4E676.html>.

[Nilsson/Lindskog/Fischer-Hübner 2001] Mikael Nilsson, Helena Lindskog, Simone Fischer-Hübner: Privacy Enhancements in the Mobile Internet; Proceedings of the IFIP WG 9.6/11.7 working conference on Security and Control of IT in Society, Bratislava, 15-16 June 2001.

[OpenGroup 2002] The Open Group: Identity Management Business Scenario; 2002; <http://www.opengroup.org/downloads/bus-scenario-IM.pdf>.

[Pescatore/Litan 2003] John Pescatore, Avivah Litan: Gartner FirstTake – Security Flaw Shows Microsoft Passport Identities Can't Be Trusted; 15 May 2003; <http://www3.gartner.com/resources/114900/114948/114948.pdf>.

[Pfitzmann 1999] Andreas Pfitzmann: Datenschutz durch Technik; in: Helmut Bäumler, Albert von Mutius (Eds.): Datenschutzgesetze der dritten Generation, Texte und Materialien zur Modernisierung des Datenschutzrechts; Neuwied 1999, 18-27.

[Pfitzmann 2001a] Andreas Pfitzmann: Entwicklung der Informations- und Kommunikationstechnik, in: Datenschutz und Datensicherheit (DuD), 25/4 (2001); Vieweg, Wiesbaden 2001; 194-195.

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

[Pfitzmann 2003] Birgit Pfitzmann: Privacy in Enterprise Identity Federation – Policies for Liberty Single Signon; in: Roger Dingledine (Ed.): Proceedings of Privacy Enhancing Technologies workshop (PET 2003); LNCS 2760; Springer, Heidelberg 2003; 189-204; <http://petworkshop.org/2003/preproc/13-preproc.pdf>; preliminary version: IBM Research Report RZ 3470 (# 93909), December 2002.

---

[Pfitzmann/Köhntopp 2001] Andreas Pfitzmann, Marit Köhntopp: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology; Draft v0.14, 2003, [http://freehaven.net/anonbib/papers/Anon\\_Terminology\\_v0.14.pdf](http://freehaven.net/anonbib/papers/Anon_Terminology_v0.14.pdf). V0.8 in H. Federrath (Ed.), Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability. LNCS 2009; 2001; 1-9.

[Pfitzmann/Pfitzmann/Schunter/Waidner 1999] Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trustworthy User Devices; in Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications, Vol. 3: Technology, Infrastructure, Economy; Addison-Wesley, München 1999; 137-156.

[Pfitzmann/Schill/Westfeld et al. 1998] Andreas Pfitzmann, Alexander Schill, Andreas Westfeld, Guntram Wicke, Gritta Wolf, Jan Zöllner: A Java-based distributed platform for multilateral security; IFIP/GI Working Conference "Trends in Electronic Commerce", June 1998, Hamburg, LNCS 1402; Springer, Berlin 1998; 52-64.

[Pfitzmann/Waidner/Pfitzmann 1990] Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; in: Datenschutz und Datensicherung (DuD) 14/5-6 (1990); Vieweg, Wiesbaden 1990; 243-253, 305-315.

[Pfitzmann/Waidner/Pfitzmann 2000] Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity. IBM Research Report RZ 3232 (#93278) 05/22/00, IBM Research Division, Zürich, May 2000; [http://www.semper.org/sirene/pointers\\_complete.html](http://www.semper.org/sirene/pointers_complete.html).

[Pfitzmann/Waidner 2002a] Birgit Pfitzmann, Michael Waidner: Research Report – Token-based Web Single Signon with Enabled Clients; 11 April 2002; <http://www.zurich.ibm.com/security/publications/2002/PfiWai2002c-TokenBased-rz3458.pdf>.

[Pfitzmann/Waidner 2002b] Birgit Pfitzmann, Michael Waidner: Privacy in Browser-Based Attribute Exchange; ACM Workshop on Privacy in the Electronic Society (WPES '02); Proceeding of the ACM workshop on Privacy in the Electronic Society; Washington, 2002; 52-62; preliminary version: IBM Research Report RZ 3412 (# 93644), June 2002.

[Pfitzmann/Waidner 2002c] Birgit Pfitzmann, Michael Waidner: BBAE – A General Protocol for Browser-based Attribute Exchange; IBM Research Report RZ 3455 (#93800), September 2002.

[Pfitzmann/Waidner 2002d] Birgit Pfitzmann, Michael Waidner: Token-based Web Single Signon with Enabled Clients; IBM Research Report RZ 3458 (#93844), November 2002.

[Pfitzmann/Waidner 2003] Birgit Pfitzmann, Michael Waidner: Federated Identity-Management Protocols – Where User Authentication Protocols May Go; accepted for 11<sup>th</sup> Cambridge International Workshop on Security Protocols, Cambridge (UK), April 2003.

[PS 2003] Microsoft: Building trust in Internet privacy: The New .NET Passport; 2003; <http://www.microsoft.com/emea/publicAffairs/positionPapers/whitePapers.mspx>.

[Popper 1973] Karl R. Popper: Objektive Erkenntnis, Hoffmann + Campe Verlag, Hamburg 1973.

[PWC 2002] PWC: E(Health) Transformation: Managing healthcare in a networked world; 2002; [http://www.kmadvantage.com/docs/km\\_articles/eHealth\\_Transformation.pdf](http://www.kmadvantage.com/docs/km_articles/eHealth_Transformation.pdf).

[Rannenberg/Pfitzmann/Müller 1996] Kai Rannenberg, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige Sicherheit; in: it+ti 4/1996, 7; revised as: IT Security and

- Multilateral Security; in: Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications, Vol. 3: Technology, Infrastructure, Economy; Addison-Wesley, München 1999; 21-29.
- [Reinhold 1991] Gerd Reinhold (Ed.): Soziologie-Lexikon; Oldenbourg Verlag, München/Wien 1991.
- [Resnick/Zeckhauser/Friedman/Kuwabara 2000] Paul Resnick, Richard Zeckhauser, Eric Friedman, Ko Kuwabara: Reputation Systems; Communications of the ACM, 43(12), December 2000; 45-48.
- [Roßnagel/Scholz 2000] Alexander Roßnagel, Philip Scholz: Datenschutz durch Anonymität und Pseudonymität; in: Multimedia und Recht (MMR); 2000(12); Verlag C.H. Beck, München 2000; 721-732.
- [Roßnagel 2002] Alexander Roßnagel: Rechtliche Unterschiede von Signaturverfahren; in: Multimedia und Recht (MMR); 2002; Verlag C.H. Beck, München 2002; 215.
- [van Rossum/Gardeniers/Borking et al. 1995] H. van Rossum, H. Gardeniers, J. Borking et al.: Privacy-Enhancing Technologies: The Path to Anonymity, Volume I u. II, Achtergrondstudies en Verkenningen 5a/5b; Registratiekamer, The Netherlands & Information and Privacy Commissioner/Ontario, Canada, August 1995; <http://www.ipc.on.ca/>.
- [RSA 2002] RSA: Identity Management: Providing Security, Convenience and Opportunity for Users and e-Businesses; Whitepaper; <http://www.rsasecurity.com/products/>.
- [Rudè 1911] G. E. Rudè: Lo Scoppio della Rivoluzione Francese in Storia del Mondo Moderno, Cambridge University Press 1911 1913, Garzanti 1978, vol. VIII; 856.
- [Ruiz 2002] Arangio-Ruiz: Istituzioni di diritto romano; Novene 2002, 426-433.
- [Savigny 1888] F. C. von Savigny: Sistema del diritto romano attuale; UTET, 1888, II, 244, 284.
- [Schetsche 2001] Michael Schetsche: Eine "neue soziale Welt" – Vorüberlegungen zu einer Mikrosoziologie des Cyberspace; 2001; <http://www1.uni-bremen.de/~mschett/sozialewelt.html>.
- [Schicker 2001] Stefan Schicker: Die elektronische Signatur; JurPC Web-Dok. 139/2001; <http://www.jurpc.de/aufsatze/20010139.htm>.
- [Schneier 1996] Bruce Schneier: Applied Cryptography; 2<sup>nd</sup> Edition; John Wiley & Sons, New York 1996.
- [Scialoja 1932] V. Scialoja: Studi giuridici, vol. III; Rome 1932; 56.
- [Shneiderman 1998] Ben Shneiderman: Designing the User Interface: Strategies for Effective Human-Computer Interaction; 3<sup>rd</sup> edition; Addison-Wesley, Boston 1998; <http://ijhcs.open.ac.uk/shneiderman/shneiderman.html>.
- [Siegel 1999] David Siegel: Futurize your Enterprise – Business Strategy in the Age of the E-Customer; John Wiley & Sons, New York 1999.
- [Simmel 1984] Georg Simmel: Grundfragen der Soziologie –Individuum und Gesellschaft, 4<sup>th</sup> edition; de Gruyter, Berlin/New York 1984 (in 1917 published for the first time).
- [Slemko 2001] Marc Slemko: Microsoft Passport to Trouble; 5 November 2001; <http://alive.znep.com/~marcs/passport/>.

---

[Smith/Mackie 2000] Eliot R. Smith, Diane Mackie: Social Psychology; 2<sup>nd</sup> edition; Worth Publishers, New York 2000.

[Spagnesi 1978] Spagnesi: item: Nome (storia); in: Enc. Dir., Vol. XXVIII, Milan 1978; 293.

[Stubblebine/Syverson 2000] Stuart Stubblebine, Paul Syverson: Authentic Attributes with Fine-Grained Anonymity Protection; Financial Cryptography 2000, LNCS Series; Springer, Berlin 2000.

[Tadelis 1999] Steven Tadelis: What's in a Name? Reputation as a Tradeable Asset; American Economic Review; Vol. 89 (3); 1999; 548-563.

[Turkle 1995] Sherry Turkle: Life on the Screen – Identity in the Age of the Internet; Simon & Schuster, New York 1995.

[US 2000] United States Senate Committee on the Judiciary: Know the Rules, Use the Tools – Privacy in the Digital Age: A Resource for Internet Users; Senator Orrin G. Hatch, Utah, Chairman Prepared by Majority Staff September 20, 2000; <http://www.senate.gov>.

[Warren/Brandeis 1890] Samuel D. Warren, Louis D. Brandeis: The Right to Privacy, 4 Harv. L. Rev. 1890.

[Warwick 2002] Kevin Warwick: Identity and Privacy Issues raised by Biomedical Implants; in: IPTS Report 67; JRC Seville, September 2002; 29-34; <http://www.jrc.es/pages/iptsreport/vol67/english/IPT5E676.html>.

[Winfield 1925] P. H. Winfield: The Chief Sources of English Legal History; Cambridge 1925.

[Wolf/Pfitzmann 1999] Gritta Wolf, Andreas Pfitzmann: Empowering Users to Set Their Protection Goals; in: Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications; Vol. 3: Technology, Infrastructure, Economy; Addison-Wesley, München 1999; 113-135.

[Wolf/Pfitzmann 2000] Gritta Wolf, Andreas Pfitzmann: Properties of protection goals their integration into user interface; Computer Networks 32 (2000); Elsevier, North-Holland 2001; 685-699.

[Zehentner 2002] Johann Zehentner: Privatheit bei Anwendungen für Identitätsmanagement im Internet / Privacy in Applications for Identity Management on the Internet; Diploma Thesis; Fakultät für Informatik der Technischen Universität München; Informatik XI: Angewandte Informatik / Kooperative Systeme; December 2002; <http://www11.in.tum.de/publications/pdf/da-zehentne2002.pdf>.

## GLOSSARY

API	Application Programming Interface
ATUS	A Toolkit for Usable Security
BGB	Bürgerliches Gesetzbuch
BVerfGE	Bundesverfassungsgerichtsentscheidung
CPEX	Global Standards for Privacy-enabled Customer Data Exchange
CPU	Central Processing Unit
DRIM	Dresden Identity Management
DRM	Digital Rights Management
ECHR	European Convention for the Protection of Human Rights
EU	European Union
GUI	Graphical User Interface
GUID	Globally Unique Identifier
ICT	Information and Communications Technologies
ID	Identity / Identifier
IEEE	Institute of Electrical and Electronics Engineers
IM	Identity Management
IMA	Identity Management Application
IMP	Identity Management Protocol
IMS	Identity Management Systems
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
LA	Liberty Alliance
LAN	Local Area Network
MAC	Media Access Control
MUD	Multi-User Dungeon
NGO	Non-Governmental Organisation
P3P	Platform for Privacy Preferences
PA	Personal Agent
PD	Pseudonym Domain
PERT	Privacy Emergency Response Team
PET	Privacy Enhancing Technology
PID	Pseudo Identity Domain
PIM	Privacy and Identity Management
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PSN	Processor Serial Number
PUID	Passport user ID
RAPID	Roadmap for Advanced Research in Privacy and Identity Management
R&D	Research and Development
REGTP	Regulierungsbehörde für Telekommunikation und Post
RFID	Radio Frequency IDentity
RTD	Research and Technological Development
SigG	Signaturgesetz
SigV	Signaturverordnung
SSONET	Security and Privacy in Open Networks
TAM	Technology Acceptance Model
TPM	Trusted Platform Module
TTF	Task-Technology Fit
URI	Uniform Resource Identifier
VwVerfG	Verwaltungsverfahrensgesetz



## ANNEXES

### 1 QUESTIONNAIRE

#### 1.1 Form Letter and Questionnaire

Kiel, 2003-04-02

Dear <Participant>,

My name is Marit Hansen. I am working for the Independent Centre for Privacy Protection Schleswig-Holstein, Germany (<http://www.datenschutzzentrum.de>).

Within the context of the project study "Identity Management Systems (IMS): Identification and Comparison Study" commissioned by the EU, IPTS Seville, the ICPP is conducting a survey with experts.

We have selected you as an expert who deals with the topic Identity Management Systems (IMS) or could presumably do so. A technically supported identity management can be a user-friendly solution to realise the demands of standardised communication between, e.g., authorities and citizens or vendors and customers. From a user's perspective, identity management can be defined as managing of own partial identities according to specific situations and contexts. The questionnaire will deal with questions about the desired range of functionality, security and privacy protection of an IMS.

With the questionnaire we would like to learn what is your point of view on identity management as an expert, and not as a representative of your organisation. The ICPP assures you that any collected data will only be used for the aforementioned research purpose. No data that might allow a relation to a certain individual or organisation will be passed on to 3rd parties. The evaluation of the questionnaire will be conducted in anonymised form.

Completing it shouldn't last longer than 20 minutes at most (18 seconds per item). Those that complete the questionnaire will receive the results of the survey and the final report of the study before its publication. Your answers should be in English, but they could be in your national language if necessary.

Yours sincerely

Marit Hansen

==

[marit.hansen@datenschutzzentrum.de](mailto:marit.hansen@datenschutzzentrum.de)

Tel: +49 431 9881214

Fax: +49 431 9881223

Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein  
Holstenstraße 98

D-24103 Kiel

Germany

---

=====

QUESTIONNAIRE

Please return - not later than 09.04.2003 - the completed questionnaire to the following address:

---

quest\_ims@datenschutzzentrum.de

A Reply-To e-mail header to this address has been set. Therefore, if you use the reply function of your e-mail client, your answer should already be addressed correctly.

You also can fax the questionnaire to this fax number:

+49 431 9881223

- 1) Do not delete any predefined text in the questionnaire.
- 2) Insert your answers only between the predefined square brackets.
- 3) Do not use square brackets or double sharps ("##") in your answers.
- 4) In case you select "other", you are welcome to note your answer between the following square brackets.

At the end of the questionnaire you have the opportunity to add an arbitrary comment regarding the questionnaire or the topic.

If you have further questions you can reach us at the following address: quest\_support@datenschutzzentrum.de

For now: Thanks you very much in advance for your support.

Yours sincerely  
Marit Hansen

#NO=====  
BACKGROUND

-----  
#V1

For how many years have you been dealing with the topic IMS?  
I have been dealing with this topic ...

- not at all
- less than few months
- less than 2 years
- less than 4 years
- less than 6 years
- less than 8 years
- less than 10 years
- since 10 years or more

-----  
#V2

How many employees are working at your organisation?

- I don't work for any organisation (freelance/self employed)
- 2 to 10 employees
- 11 to 25 employees
- 26 to 50 employees
- 51 to 100 employees
- 101 to 250 employees
- more than 250 employees

-----  
#V3

What is your organisation's primary relationship towards the topic of IMS?

- We are a manufacturer/distributor of an IMS.
- We are a user of an IMS.
- We conduct research at university.
- We work as journalists/authors/publicists.

- [ ] We are a group defending citizens' and consumers' interests.  
 [ ] We are a privacy agency.  
 [ ] We are a law enforcement agency.  
 [ ] We are a service provider.  
 [ ] other
- #V4  
 - In case "other" please specify:  
 [ ]
- #V5  
What is your position in your organisation with reference to the topic of IMS?  
[ ] management  
[ ] marketing  
[ ] human resources management  
[ ] research  
[ ] programmer for security/functionality/usability...  
[ ] jurist  
[ ] jurist, specialised to law enforcement  
[ ] lobbyist  
[ ] user  
[ ] other
- #V6  
- In case "other" please specify:  
[ ]
- #V7  
Do you already use an IMS?  
[ ] Yes  
[ ] No  
- In case "Yes":
- #V8  
For which application(s)?  
[ ]
- #V9  
With which product(s)?  
[ ]
- What are your interests regarding IMS? I am particularly interested in ...
- #V10  
... range of functions:  
[ ] not at all [ ] [ ] [ ] [ ] very
- #V11  
... usability:  
[ ] not at all [ ] [ ] [ ] [ ] very
- #V12  
... privacy protection:  
[ ] not at all [ ] [ ] [ ] [ ] very
- #V13  
... security:  
[ ] not at all [ ] [ ] [ ] [ ] very

---

#V14  
... marketability (in terms of "people will be ready to pay for it"):  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V15  
... politically pushing through:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V16  
... politically preventing it:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V17  
... implementing law:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V18  
... social impacts of the implementation/use:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V19  
... potential psychological consequences:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V20  
... law enforcement:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V21  
... access rights management:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V22  
... multiple application usage:  
[ ] [ ] [ ] [ ]  
not at all [ ] very

#V23  
If you think on another important category, please specify:  
[ ]

#V24  
[ ] [ ] [ ] [ ]  
not at all [ ] very

-----  
#V25  
Which country would best describe your cultural background?  
[ ]

=====

STATE-OF-THE-ART, TRENDS and RATINGS

-----  
#V26

Which already working IMS would you call state-of-the art?  
Please specify the name(s) of the product(s) with a short statement.

[ ]

-----  
#V27

What do you consider should be the essential function(s) of an IMS?

[ ]

-----  
#V28

How do you assess the current marketability (in terms of "people will be ready to pay for it") of IMS?

- [ ] very bad
- [ ] bad
- [ ] indifferently
- [ ] good
- [ ] very good
- [ ] I don't know.

-----  
#V29

How do you assess the marketability (in terms of "people will be ready to pay for it") of IMS in ten years?

- [ ] very bad
- [ ] bad
- [ ] indifferently
- [ ] good
- [ ] very good
- [ ] I don't know.

-----  
#V30

What do you think, how long will it take for a society-wide implementation of a multi-purpose IMS for every day use?

[ ]

-----  
#V31

Which aspects of an IMS are particularly important for a use on a grand scale within society (general acceptance, deployment)?

range of functions

- |           |     |     |     |           |
|-----------|-----|-----|-----|-----------|
| [ ]       | [ ] | [ ] | [ ] | [ ]       |
| not       |     |     |     | very      |
| important |     |     |     | important |

#V32

multi-purpose usage

- |           |     |     |     |           |
|-----------|-----|-----|-----|-----------|
| [ ]       | [ ] | [ ] | [ ] | [ ]       |
| not       |     |     |     | very      |
| important |     |     |     | important |

#V33

usability

- |           |     |     |     |           |
|-----------|-----|-----|-----|-----------|
| [ ]       | [ ] | [ ] | [ ] | [ ]       |
| not       |     |     |     | very      |
| important |     |     |     | important |

#V34

privacy protection

- |     |     |     |     |     |
|-----|-----|-----|-----|-----|
| [ ] | [ ] | [ ] | [ ] | [ ] |
|-----|-----|-----|-----|-----|

---

<p>not important</p> <p>#V35</p> <p>security</p> <p>[ ]                  [ ]                  [ ]                  [ ]</p> <p>not important</p>	<p>very important</p> <p>very important</p>
---	---

<p>#V36</p> <p>cost</p> <p>[ ]                  [ ]                  [ ]                  [ ]</p> <p>not important</p>	<p>very important</p>
--	---------------------------

<p>#V37</p> <p>controllability for users</p> <p>[ ]                  [ ]                  [ ]                  [ ]</p> <p>not important</p>	<p>very important</p>
---	---------------------------

<p>#V38</p> <p>controllability for government</p> <p>[ ]                  [ ]                  [ ]                  [ ]</p> <p>not important</p>	<p>very important</p>
--	---------------------------

<p>#V39</p> <p>tracing of law enforcement respectively prosecution of claim?</p> <p>[ ]                  [ ]                  [ ]                  [ ]</p> <p>not important</p>	<p>very important</p>
---	---------------------------

<p>#V40</p> <p>If you think on another category, please specify: [ ]</p>
--

<p>#V41</p> <p>[ ]                  [ ]                  [ ]                  [ ]</p> <p>not important</p>	<p>very important</p>
--	---------------------------

---

<p>#V42</p> <p>Should the administration of personal data collected by an IMS be conducted by the user himself/herself or by a central instance?</p> <p>[ ] Administration of personal data should be as centralised as possible by organisations.</p> <p>[ ] Administration of personal data should be as decentralised as possible by the users themselves.</p> <p>[ ] other</p>
--

<p>#V43</p> <p>- In case "other" please specify: [ ]</p>
--

---

<p>OPERATIONAL GAPS</p>	
-------------------------	--

---

<p>#V44</p> <p>Do you think that there could be psychological consequences as a result of the use of IMS?</p> <p>[ ] No</p> <p>[ ] Yes</p> <p>- In case "Yes" please specify:</p>
---

#V45

#V46

Will an IMS improve or worsen the following aspects of law enforcement respectively prosecution of claim?

liability

- worsen
- no change
- improve
- I don't know.

#V47

crime prosecution

- worsen
- no change
- improve
- I don't know.

#V48

clarification of facts

- worsen
- no change
- improve
- I don't know.

#V49

probative value of admissible evidence

- worsen
- no change
- improve
- I don't know.

#V50

If you think on another important category, please specify:

#V51

- worsen
- no change
- improve
- I don't know.

#V52

Which of the following aspects do you foresee as a potential main bottleneck regarding mass adoption of IMS?

- bad usability
- insufficient technological development of a society-wide infrastructure for an IMS
- insufficient security
- insufficient privacy protection
- too weak law enforcement
- too strong law enforcement
- too expensive

#V53

If you think on other issues/bottlenecks, please specify:

#V54

What are the texts which you consider most significant or visionary to IMS? Please give 1-3 references.

[ ]

-----  
#V55

If you have already published articles or programs  
concerning IMS: Please list your most important ones.

[ ]

-----  
#V56

In case you'd like to leave a comment regarding the questionnaire  
or the topic of IMS in general, please do so.

[ ]

## 1.2 Results

### FREQUENCIES

VARIABLES=v1 v2 v3 v4 v5 v6 v7 v8 v9 v10 v11 v12 v13 v14 v15 v16 v17 v18  
v19 v20 v21 v22 v23 v24 v25 v26 v27 v28 v29 v31 v32 v33 v34 v35 v36 v37 v38  
v39 v40 v41 v42 v43 v44 v45 v46 v47 v48 v49 v50 v51 v52 v53 v54 v55 v56 v57  
v58 v59  
/ORDER= ANALYSIS .

**Table 34: V1 – How Many Years Dealing with IMS...**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	10	11.2	11.2	11.2
	Less than few months	7	7.9	7.9	19.1
	Less than 2 years	19	21.3	21.3	40.4
	Less than 4 years	30	33.7	33.7	74.2
	Less than 6 years	5	5.6	5.6	79.8
	Less than 8 years	7	7.9	7.9	87.6
	Less than 10 years	3	3.4	3.4	91.0
	Since 10 years or more	8	9.0	9.0	100.0
	Total	89	100.0	100.0	

**Table 35: V2 – Employees in Organisation ...**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No work for organisation	6	6.7	6.7	6.7
	2 to 10 employees	10	11.2	11.2	18.0
	11 to 25 employees	11	12.4	12.4	30.3
	26 to 50 employees	13	14.6	14.6	44.9
	51 to 100 employees	8	9.0	9.0	53.9
	101 to 250 employees	4	4.5	4.5	58.4
	> 250 employees	37	41.6	41.6	100.0
	Total	89	100.0	100.0	

**Table 36: V3 – Organisation and IMS ...**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Manufacturer / distributor of IMS	11	12.4	12.8	12.8
	User of IMS	2	2.2	2.3	15.1
	Research at university	29	32.6	33.7	48.8
	Defending citizens' / customers' interests	3	3.4	3.5	52.3
	Privacy agency	16	18.0	18.6	70.9
	Law enforcement agency	6	6.7	7.0	77.9
	Service provider	1	1.1	1.2	79.1
	Other	18	20.2	20.9	
	Total	86	96.6	100.0	
	Missing	98	3	3.4	
Total		89	100.0		

**Table 37: V4 – Other Organisation ...**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Data protection	2	2.2	9.1	9.1
	Pressure group / Standardisation	4	4.5	18.2	27.3
	Research	8	9.0	36.4	63.6
	Company / attorney	5	5.6	22.7	86.4
	User	2	2.2	9.1	95.5
	Misc.	1	1.1	4.5	
	Total	22	24.7	100.0	
	Missing	8	67	75.3	
Total		89	100.0		

**Table 38: V5 – Position in Organisation ...**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Management	13	14.6	14.8	14.8
	Marketing	3	3.4	3.4	18.2
	Research	46	51.7	52.3	70.5
	Programmer for security / functionality / usability ...	2	2.2	2.3	72.7
	Jurist	6	6.7	6.8	79.5
	Jurist specialised to law enforcement	1	1.1	1.1	80.7
	Lobbyist	3	3.4	3.4	84.1
	User	1	1.1	1.1	85.2
	Other	13	14.6	14.8	
	Total	88	98.9	100.0	
	Missing	98	1	1.1	
	Total	89	100.0		

**Table 39: V6 – Other Position ...**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	(Project-) Management	8	9.0	38.1	38.1
	Pressure group	1	1.1	4.8	42.9
	Consulting	1	1.1	4.8	47.6
	Research	3	3.4	14.3	61.9
	Technician. programmer	3	3.4	14.3	76.2
	Misc.	5	5.6	23.8	100.0
	Total	21	23.6	100.0	
Missing	0	1	1.1		
	8	67	75.3		
	Total	68	76.4		
	Total	89	100.0		

**Table 40: V7 – Do You Already Use an IMS?**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	25	28.1	28.4	28.4
	No	63	70.8	71.6	100.0
	Total	88	98.9	100.0	
Missing	8	1	1.1		
	Total	89	100.0		

**Table 41: V8 – For Which Application?**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	General applications	10	11.2	45.5	45.5
	More specialised applications	3	3.4	13.6	59.1
	IM specialised applications	1	1.1	4.5	63.6
	Management of members	4	4.5	18.2	81.8
	Misc.	4	4.5	18.2	100.0
	Total	22	24.7	100.0	
	Total	89	100.0		
Missing	8	67	75.3		
	Total	89	100.0		

General applications (1)

- "Web, e-mail"
- "internet browser"
- "email and web"
- "Probably not an IMS in your sense, but several enterprise collaboration tools we are using have aspects of an IMS"
- "E-mail, authentication"
- "Not sure if this counts, but my Mozilla keeps track of accounts, passwords, etc for me"
- "most of the office applications"
- "Websurfing"
- "mailing, networking"
- "Web browsing"

More specialised applications (2)

- "email, address book, authentication/authorisation for business applications"
- "identification, access rights management, secure email"
- "I use several very limited IMS, offering use of different accounts and pseudonyms (but not providing real management support; e.g. e-mail, accessing (personalised) web sites"

IM specialised applications (3)

- "CookieCooker, Passport"

Management of members (4)

- "Access control to IT University wireless network"
- "Customer Relationship Management"
- "human resource management"
- "Part of our infrastructure to support our members"

Misc. (5)

- "access"

- "partly Internet usage"
- "several applications"
- "mobile telephony"

**Table 42: V9 – With Which Product?**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Specialised applications for IM	14	15.7	70.0	70.0
	General applications for communication	5	5.6	25.0	95.0
	Specialised procedure	1	1.1	5.0	100.0
	Total	20	22.5	100.0	
Missing	8	69	77.5		
Total		89	100.0		

Specialised applications for IM (1)

- "jap"
- "CookieCooker (3)"
- "Netscape + Intranet based on INFORMIX"
- "Internally-developed solutions using Informix RDBMS"
- "Passport"
- "PGP, Windows PKI, .Net Passport"
- "smartcard"
- "FINEID, Teamware"
- "Self developed"
- "IBM Role Your Own"
- "Sun ONE Directory Server, migrating to Sun ONE Identity Server"
- "in-house"

General applications for communication (2)

- "Kmail, Mutt, Konqueror, Opera"
- "Lotus products"
- "GSM SIM"
- "different browsers/e-mail agents"
- "PC"

Specialised procedure (3)

- "Pseudonyms provided by ISPs"

**Table 43: V10 – Interests in IMS ... Range of Functions**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	2	2.2	2.4	2.4
	...	12	13.5	14.3	16.7
	...	26	29.2	31.0	47.6
	...	23	25.8	27.4	75.0
	Very	21	23.6	25.0	100.0
	Total	84	94.4	100.0	
Missing	8	5	5.6		
Total		89	100.0		

**Table 44: V11 – Interests in IMS ... Usability**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	...	6	6.7	7.1	7.1
	...	10	11.2	11.9	19.0
	...	31	34.8	36.9	56.0
	very	37	41.6	44.0	100.0
	Total	84	94.4	100.0	
Missing	8	5	5.6		
Total		89	100.0		

**Table 45: V12 – Interests in IMS ... Privacy Protection**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	...	1	1.1	1.1	1.1
	...	4	4.5	4.6	5.7
	...	13	14.6	14.9	20.7
	Very	69	77.5	79.3	100.0
	Total	87	97.8	100.0	
	Missing	8	2	2.2	
Total		89	100.0		

**Table 46: V13 – Interests in IMS ... Security**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	1	1.1	1.1	1.1
	...	7	7.9	8.0	9.2
	...	24	27.0	27.6	36.8
	Very	55	61.8	63.2	100.0
	Total	87	97.8	100.0	
	Missing	8	2	2.2	
Total		89	100.0		

**Table 47: V14 – Interests in IMS ... Marketability**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	14	15.7	16.5	16.5
	...	22	24.7	25.9	42.4
	...	21	23.6	24.7	67.1
	...	18	20.2	21.2	88.2
	Very	10	11.2	11.8	100.0
	Total	85	95.5	100.0	
Missing	8	4	4.5		
	Total	89	100.0		

**Table 48: V15 – Interests in IMS ... Politically Pushing Through**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	10	11.2	11.6	11.6
	...	22	24.7	25.6	37.2
	...	23	25.8	26.7	64.0
	...	20	22.5	23.3	87.2
	Very	11	12.4	12.8	100.0
	Total	86	96.6	100.0	
Missing	8	3	3.4		
	Total	89	100.0		

**Table 49: V16 – Interests in IMS ... Politically Preventing it**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	41	46.1	48.2	48.2
	...	19	21.3	22.4	70.6
	...	16	18.0	18.8	89.4
	...	4	4.5	4.7	94.1
	Very	5	5.6	5.9	100.0
	Total	85	95.5	100.0	
Missing	8	4	4.5		
	Total	89	100.0		

**Table 50: V17 – Interests in IMS ... Implementing Law**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	10	11.2	11.6	11.6
	...	26	29.2	30.2	41.9
	...	16	18.0	18.6	60.5
	...	19	21.3	22.1	82.6
	Very	15	16.9	17.4	100.0
	Total	86	96.6	100.0	
Missing	8	3	3.4		
Total		89	100.0		

**Table 51: V18 – Interests in IMS ... Social Impacts of Implementation / Use**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	4	4.5	4.6	4.6
	...	13	14.6	14.9	19.5
	...	20	22.5	23.0	42.5
	...	26	29.2	29.9	72.4
	Very	24	27.0	27.6	100.0
	Total	87	97.8	100.0	
Missing	8	2	2.2		
Total		89	100.0		

**Table 52: V19 – Interests in IMS ... Potential Psychological Consequences**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	11	12.4	12.9	12.9
	...	27	30.3	31.8	44.7
	...	15	16.9	17.6	62.4
	...	18	20.2	21.2	83.5
	Very	14	15.7	16.5	100.0
	Total	85	95.5	100.0	
Missing	8	4	4.5		
Total		89	100.0		

**Table 53: V20 – Interests in IMS ... Law Enforcement**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	13	14.6	14.9	14.9
	...	16	18.0	18.4	33.3
	...	19	21.3	21.8	55.2
	...	22	24.7	25.3	80.5
	Very	17	19.1	19.5	100.0
	Total	87	97.8	100.0	
Missing	8	2	2.2		
Total		89	100.0		

**Table 54: V21 – Interests in IMS ... Access Right Management**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	7	7.9	8.1	8.1
	...	7	7.9	8.1	16.3
	...	21	23.6	24.4	40.7
	...	22	24.7	25.6	66.3
	Very	29	32.6	33.7	100.0
	Total	86	96.6	100.0	
Missing	8	3	3.4		
Total		89	100.0		

**Table 55: V22 – Interests in IMS ... Multiple Application Usage**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	5	5.6	5.9	5.9
	...	11	12.4	12.9	18.8
	...	20	22.5	23.5	42.4
	...	23	25.8	27.1	69.4
	Very	26	29.2	30.6	100.0
	Total	85	95.5	100.0	
Missing	8	4	4.5		
Total		89	100.0		

**Table 56: V23 – Interests in IMS ... Another Important Category**

	Frequency	Percent
Missing	8	100.0

**Table 57: V24 – Interests in IMS ... Another Important Category**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	2	2.2	16.7	16.7
	...	1	1.1	8.3	25.0
	Very	9	10.1	75.0	100.0
	Total	12	13.5	100.0	
	Missing	8	77	86.5	
	Total		89	100.0	

**Table 58: V25 – Cultural Background**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Europe	2	2.2	2.6	2.6
	Austria	1	1.1	1.3	3.9
	Czech Republic	1	1.1	1.3	5.3
	Denmark	1	1.1	1.3	6.6
	Finland	1	1.1	1.3	7.9
	France	3	3.4	3.9	11.8
	Germany	26	29.2	34.2	46.1
	Greek	1	1.1	1.3	47.4
	Italy	3	3.4	3.9	51.3
	Moldavia	1	1.1	1.3	52.6
	Nether- lands	5	5.6	6.6	59.2
	Spain	2	2.2	2.6	61.8
	Switzerland	5	5.6	6.6	68.4
	UK	6	6.7	7.9	76.3
	Canada	3	3.4	3.9	80.3
	USA	11	12.4	14.5	94.7
	Africa	1	1.1	1.3	96.1
	Australia	1	1.1	1.3	97.4
	Japan	2	2.2	2.6	100.0
	Total	76	85.4	100.0	
Missing	98	13	14.6		
Total		89	100.0		

**Table 59: V26 – IMS – State-of-the-Art**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Specified product	16	18.0	47.1	47.1
	Passport	8	9.0	23.5	70.6
	None	8	9.0	23.5	94.1
	No idea / no experience	2	2.2	5.9	100.0
	Total	34	38.2	100.0	
Missing		8	55	61.8	
	Total		89	100.0	

## Application (1)

- "XMCARE from ICL/Simac for more information Mr Gilles van Blarkom +31703811308"
- "Network Identity of SUN Microsystems"
- "Pseudonyms provided by ISPs, anonymous proxies such as JAP, MIX networks such as Crowds"
- "jap, the only one I ever used"
- "In-enterprise single signon and collaboration tools for employees. In-enterprise personalization tools for customers. Browser personalization. Microsoft Passport. Gator. Zero-knowledge. Roboform. Passlogix."
- "TIVOLY – good, Oblix – interesting, CA eTrust – big market, PKI-services/ products – not user friendly"
- "Passport – they are still resolving legal and technical issues, I know of no adequate one."
- "Anonymizer"
- "I don't know of any good ones for protecting privacy that are fielded, but Stefan Brands "private credentials" design is most advanced."
- "The Parkinsonpas, a project in the Dutch City of Alphen a/d Rijn. By means of a chipcard combined with biometrics patients can personally decide to offer insight to their medical records to different medical agencies. Besides, the chipcard timely warns the patient to take his or her medicine"
- "We have own solutions and we have used it some products; ID2, FINEID, and so on"
- ".Net; Liberty Alliance; ZeroKnowledge; biometric technologies may – be of assistance if used the right way – see OECD work here"
- "Anonymisieren (AN.ON) P3P PGP, soweit Schutz gegen Dritte "
- "Without privacy: Passport, Liberty Alliance, Addressing Privacy/self-determination: P3P implementations such as AT&T's Privacy Bird"
- "Our implementation of IMS for a specific customer"
- "Sun ONE Identity Server 6.0"
- "Liberty Alliance is beginning to work."
- "Netegrity Identity + Access Management System"
- "Verisign – digital signature certification"

## Passport (2)

- "Passport: most common system"
- Microsoft Passport (4x)

## None (3)

- "none of those I know or have read about; BTW: often the term is used in what I would call a "reversed" way, IM is the thing that allows network & system administrators to manage users and their access rights"
- "none", "no existing" (3x)
- "I don't think there are any IMS today, which are state of the art."
- "don't know any!"
- "Are there any "State of the Art"?"
- "I am not aware of any IMS product on the market, which could be called state-of-the-art."
- "Typical e-mail clients and browsers (e.g., Mozilla); also Microsoft Passport (reminder: I don't think that there is an already working IMS which fulfills relevant criteria)"

## Don't know, no idea (4)

- "Not familiar enough with the field"
- "no experience"

**Table 60: V27 – IMS – Essential Functions ...**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Generic functions in a more general sense	19	21.3	30.2	30.2
	Generic functions in a more specified sense	20	22.5	31.7	61.9
	Specific functions with an operational oriented perspective	21	23.6	33.3	95.2
	Misc.	3	3.4	4.8	100.0

	Total	63	70.8	100.0	
Missing	8	26	29.2		
Total		89	100.0		

Generic functions in a more general sense (1)

- "Privacy Protection" (8x)
- "identity protection"
- "security" (6x)
- "anonymisation"
- "pseudonymity" (2x)
- "Persönlichkeitsschutz"
- "ease of use" (2x)
- "range of functions"
- "Ensure protection and privacy of personally identifiable information."
- "Empower people and enable products"
- "Linking the real world to the digital world without misusing identity"
- "Security – Cost reduction"
- "data protector"

Generic functions in a more specified sense (2)

- "management of pseudonyms"
- "Providing multiple applications with personal data."
- "integration with applications."
- "Manage the virtual identities of the user. This should be done in a secure way, and protecting the privacy of the user."
- "universal compatibility"
- "permitting the user to execute his right to informational self-determination; I am aware of the fact that this is a very high-level description – probably too high to be considered a function; my only excuse is that I have so far not seen anything that would merit being called an IMS."
- "multiple identities if necessary; anonymity/pseudonymity if possible; minimal data exchange & data trails where not."
- "it should help me to organise all my social relationships in a secure and privacy-protected form."
- "Trust"
- "Protection of identity (and privacy) against third parties"
- "hide the linkage between my identity and my thoughts/ interests/ work"
- "anonymous/pseudonymous use, unlinkability"
- "Lie."
- "role management, user control of personal data, preferences management, user friendly interfaces, analysis and education"
- "correct, pervasive role changes on command and ease of use"
- "Remembering what it has been told and who to release it to"
- "PROVISION OF ANONYMITY/AliasING RELATED WITH GUARANTEED PRIVACY, SECURITY AND CONFIDENTIAL DISCLOSURE OF ANONYMITY/AliasING UNDER WELL DEFINED CIRCUMSTANCES."
- "facilitate online transactions"
- "practical, useful, not too expensive, secure, standard product, co-operation"
- "Clear user interface; comprehensive approach to personal data"
- "Allowing a user to manage his or her own identities (plural meant), and to track and understand how others are using those identities"
- "Secure informational self-determination for data subjects"

Specific functions with an operational oriented perspective (3)

- "hiding personal data, negotiation of data disclosure, authentication, authorisation via credentials."
- "identity editor, anonymity service"
- "Single Sign-On"
- "minimization of personal data, unlinkability"
- "Management of Pseudonyms, Anonymity, Digital Signatures"
- "Caching decisions of the user once made in a certain context and remembering which information was left where."
- "Absence of single point of control. Possibility of multiple identity providers for each person, including the person itself. Privacy, meaning that all released data can be governed by policy, and a reasonable policy-management system, including user choices where not prescribed otherwise by existing regulations or contracts. Security. -- Remark: I see marketability initially as a B2B case, and thus marketability as a question of what it initially offers to the participating enterprises. Hence I answer the next questions with respect to \*enterprises\* installing and paying for these systems, not end users as the authors may have meant."
- "Let the user choose different roles for different actions – prevent dissemination of personal data, if the user wants it – Manage certified data items, i.e., driving licence, digital ID card – (not really a function, but very important:) usability for unexperienced persons."
- "linking persons to identities in an unforgeable way, separating application domains, managing credentials"
- "Proofs of Compliance to stated Policies"
- "automatic pseudonym switching according to context"
- "Data Protection compliant – e.g., facilitating fulfilment of subject access request, privacy protection against linkability or correlation of behaviour without consent"
- "Conveniently allows users to control distribution of information to vendors/web sites"
- "Avoid need for user to enter multiple passwords and usernames while maintaining a controllable level of anonymity and keeping use of pseudonyms under user control"
- "highly reliable identity authentication"
- "independent pseudonyms (identities) for different contacts or applications; automatic, transparent and reliable identification with suitable roles; easy control over information contained in a communicated pseudonym"
- "Provide unlinkability between users activities in the Internet and their identity"

- "Integration and Linkability Control"
- "Support for Authentication, Authorisation, Auditability, Distributed Identity and Interoperability – preferably via open standards"
- "Management of multiple (partial) identities, end-user control, anonymity, linkability control"
- "user-controlled linkability; creation, use and choice of pseudonyms and related data sets (including certificates, attributes, credentials); context detection; configuration of rules to decide on roles/context and thus, (re-)use of pseudonyms; history function (transaction logging and interpretation); other support for the user to help him in privacy-enhancing management of his identities; privacy and security baseline (e.g. providing anonymity/unobservability in the communication network, crypto functionality for confidentiality and integrity (e.g. encryption, digital signatures incl. PKI), protection of the IMS itself against attacks); appropriate IMS infrastructure including specific IM-related services (e.g. identity brokers ...)"

Misc. (4)

- "I have not been informed of your definition of IMS."
- "added value in service delivery from a user-perspective"
- "It should not be used as if it does more than it is technically capable of doing."

**Table 61: V28 – IMS – Marketability**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very bad	11	12.4	12.8	12.8
	Bad	31	34.8	36.0	48.8
	Indifferently	25	28.1	29.1	77.9
	Good	8	9.0	9.3	87.2
	I don't know	11	12.4	12.8	100.0
	Total	86	96.6	100.0	
	Missing	8	3	3.4	
Total		89	100.0		

**Table 62: V29 – IMS – Marketability in 10 Years**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very bad	2	2.2	2.3	2.3
	Bad	5	5.6	5.8	8.1
	Indifferently	18	20.2	20.9	29.1
	Good	32	36.0	37.2	66.3
	Very good	10	11.2	11.6	77.9
	I don't know	19	21.3	22.1	100.0
	Total	86	96.6	100.0	
	Missing	8	3	3.4	
	Total	89	100.0		

**Table 63: V30 – How Long Will it Take for a Society-Wide Implementation of a Multi-Purpose IMS?**

	N	Minimum	Maximum	Mean	Std. Deviation
V30 – How long for a society-wide implementation of IMS	58	2	50	11.55	8.738
Valid N (listwise)	58				

**Table 64: V31 – IMS – Important for Use in Society – Range of Functions**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not important	5	5.6	6.0	6.0
	...	17	19.1	20.5	26.5
	...	24	27.0	28.9	55.4
	...	22	24.7	26.5	81.9
	Very important	15	16.9	18.1	100.0
	Total	83	93.3	100.0	
	Missing	8	6	6.7	
Total		89	100.0		

**Table 65: V32 – IMS – Important for Use in Society – Multi-Purpose Usage**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not important	3	3.4	3.5	3.5
	...	5	5.6	5.8	9.3
	...	19	21.3	22.1	31.4
	...	32	36.0	37.2	68.6
	Very important	27	30.3	31.4	100.0
	Total	86	96.6	100.0	
Missing	8	3	3.4		
Total		89	100.0		

**Table 66: V33 – IMS – Important for Use in Society – Usability**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not important	1	1.1	1.2	1.2
	...	3	3.4	3.5	4.7
	...	10	11.2	11.6	16.3
	Very important	72	80.9	83.7	100.0
	Total	86	96.6	100.0	
	Missing	8	3	3.4	
Total		89	100.0		

**Table 67: V34 – IMS – Important for Use in Society – Privacy Protection**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	...	2	2.2	2.3	2.3
	...	11	12.4	12.5	14.8
	...	29	32.6	33.0	47.7
	Very important	46	51.7	52.3	100.0
	Total	88	98.9	100.0	
	Missing	8	1	1.1	
Total		89	100.0		

**Table 68: V35 – IMS – Important for Use in Society – Security**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	...	2	2.2	2.3	2.3
	...	14	15.7	15.9	18.2
	...	26	29.2	29.5	47.7
	Very important	46	51.7	52.3	100.0
	Total	88	98.9	100.0	
	Missing	8	1	1.1	
Total		89	100.0		

**Table 69: V36 – IMS – Important for Use in Society – Cost**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	...	6	6.7	6.9	6.9
	...	16	18.0	18.4	25.3
	...	36	40.4	41.4	66.7
	Very important	29	32.6	33.3	100.0
	Total	87	97.8	100.0	
	Missing	8	2	2.2	
Total		89	100.0		

**Table 70: V37 – IMS – Important for Use in Society – Controllability for Users**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	...	8	9.0	9.4	9.4
	...	15	16.9	17.6	27.1
	...	26	29.2	30.6	57.6
	Very important	36	40.4	42.4	100.0
	Total	85	95.5	100.0	
	Missing	8	4	4.5	
Total		89	100.0		

**Table 71: V38 – IMS – Important for Use in Society – Controllability for Government**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not important	11	12.4	12.9	12.9
	...	23	25.8	27.1	40.0
	...	27	30.3	31.8	71.8
	...	18	20.2	21.2	92.9
	Very important	6	6.7	7.1	100.0
	Total	85	95.5	100.0	
Missing	8	4	4.5		
	Total	89	100.0		

**Table 72: V39 – IMS – Important for Use in Society – Tracing of Law Enforcement**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not important	13	14.6	15.5	15.5
	...	12	13.5	14.3	29.8
	...	29	32.6	34.5	64.3
	...	17	19.1	20.2	84.5
	Very important	13	14.6	15.5	100.0
	Total	84	94.4	100.0	
Missing	8	5	5.6		
	Total	89	100.0		

**Table 73: V40 – IMS – Important for Use in Society – Other Category**

	Frequency	Percent
Missing	8	89

**Table 74: V41 – IMS – Important for Use in Society – Specified Category**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not important	2	2.2	16.7	16.7
	...	2	2.2	16.7	33.3
	...	1	1.1	8.3	41.7
	Very important	7	7.9	58.3	100.0
	Total	12	13.5	100.0	
	Missing	8	77	86.5	
Total		89	100.0		

**Table 75: V42 – Administration of Data**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Administration by organisation	4	4.5	4.7	4.7
	Administration by user	61	68.5	71.8	76.5
	Other	20	22.5	23.5	100.0
	Total	85	95.5	100.0	
Missing	8	4	4.5		
Total		89	100.0		

**Table 76: V43 – Administration of Data – Some Comments**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Both should do ...	8	9.0	42.1	42.1
	It depends on ...	3	3.4	15.8	57.9
	None of both. but ...	4	4.5	21.1	78.9
	Discussion and differentiation	4	4.5	21.1	100.0
	Total	19	21.3	100.0	
Missing	8	70	78.7		
Total		89	100.0		

"Both should do" (1)

- "Both should do it. Users should be able to override what central administration does."
- "General information should be administered centrally with more sensitive data being administered by the user."
- "Technology should enable both. It's on the user to decide depending on the context he is in: Think of a world of mobile devices, where info has to be stored somewhere in the network."
- "Both should be able"
- "The relation between both alternatives above should be well balanced."
- "A hybrid is probably optimal. Centralization of control is crucial to ensure good information, protect security, and even privacy of the data. That said, users need the power to ensure proper policies are enforced and retain control over how data is used, where possible."
- "Administration should be federated, allowing the user to manage their own data even if it is held by a number of third parties with whom the user has some trust relationship."
- "Decentralized, but users can only make changes that are screened."

"It depends on ..." (2)

- "It depends on the data. For example, preferences should be decentralized; names and addresses should be centralized."
- "It depends on the different value of its parts, the costs of administration, and the advantage for the user."
- "Depending on the application."

"None of both, but ..." (3)

- "By multiple independent third parties, which could be chosen by the user."
- "I think users will want numerous organizations to centralize parts of their identities, but not have any single organization knowing all about all of his or her various identities nor be responsible for all of the information his or her self."
- "Users would probably be willing to pay service providers to maintain their personal data."
- "government or banks"

Differentiations and discussions (4)

- "Under user control does not have to be clientside."
- "a) There should be a choice. It should be \*possible\* for user to do their own administration at least of data they choose themselves, and it should be made as easy as possible, but some people do prefer to have it done for them.  
b) There \*are\* data that only arise in interaction with organizations. For those the absence of single points of control is important, i.e., the data should remain in the individual organizations, and the system design should not require trust of these organizations in each other or in a central instance."
- "The priorities should be trust and security of data, followed by convenience and technical feasibility."
- "The users should decide on administration, so by default administration directly by the users themselves, but with the possibility to being supported by other parties."

**Table 77: V44 – Psychological Consequences**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	34	38.2	43.0	43.0
	Yes	45	50.6	57.0	100.0
	Total	79	88.8	100.0	
Missing	8	10	11.2		
	Total	89	100.0		

**Table 78: V45 – Specified Psychological Consequences**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	1	1.1	2.6	2.6
	Affirming the thesis	3	3.4	7.9	10.5
	More positive aspects mentioned ...	6	6.7	15.8	26.3
	More negative aspects mentioned ...	13	14.6	34.2	60.5
	Indifferent about positive or negative aspects ...	4	4.5	10.5	71.1
	Substantiating the thesis: the "role explication" aspect	6	6.7	15.8	86.8
	Misc.	5	5.6	13.2	
	Total	38	42.7	100.0	
Missing	8	51	57.3		
Total		89	100.0		

## Affirming the thesis (1)

- "too many to describe without just providing a "laundry list" – depends on actual implementation. But definitely there will be psychological and sociological consequences the more IMS will be widespread"
- "possibly yes"
- "the way we represent ourselves will evolve and will have an impact on our behaviour."

## More positive aspects mentioned (2)

- "stress levels and irritation at reduced functionality if use privacy enhancing technology"
- "Better confidence in person-to-person relations and in technology"
- "Distress from personal information being widely distributed. E.g., Clare Swire email about a year ago."
- "feeling of security and self responsibility by using the internet"
- "weariness and paranoia online should decrease slowly and slightly, as users are more in charge of who can see what they do and where they are. this is in my eyes the only reason why anybody should worry about identity management."
- "if the system is ok, so we have more trust"

## More negative aspects mentioned (3)

- "No permanent, but it is easier to "kill people without looking in their eyes". Within the grey masses, people will be and act more radical."
- "Psychologically individuals want to control their lives, if not research show people will become depressed! (provided they are aware of it. It's a matter of consciousness.)"
- "Depending on design: Feeling of loss of control. Feeling of more/less complexity in interactions. Feeling of trust/privacy."
- "There is psychological prerequisites for the usage of IMS, and as a consequence its use will have impact and consequences on the people who might use it. Awareness of surveillance but also maybe an increase sense of paranoia in others might occur."
- "The haunting feeling that somebody right now is selling your personal data, perhaps?"
- "People may not trust access management/credential-based decisions made by the IMS; people may be afraid of other parties sneakily accessing personal data."
- "1. Everything one does has psychological consequences :-) 2. People will be more aware on who knows what about them on the net, at they will use this knowledge."
- "several: loss of control, identity, responsibility"
- "I think there are important issues of control and disempowerment."
- "there should be worries about personal data protection"
- "Users are going to have to trust the IMS system(s). This is a psychological notion; the less trust there is the less use there will be and the more fear and uncertainty will be produced"
- "Potentially, users will not trust the IMS with their data unless it is clear to them what protection it offers – logical, procedural and liability"
- "Possibly being out of order an human if IMS doesn't work"

## Indifferent about positive or negative (4)

- "Complex question. It may be that people have very different propensities to divide their behaviour under different personae, or that latent propensities may emerge more widely than imagined. It may also be that greater awareness of privacy risks may not be matched by peoples ability to use protecting systems, leading to anxiety or resignation. It might stimulate emergence of interesting sub-cultures, and social engagement, but it might also have divisive tendencies. Needs lot of research, simulation and experiment."
- "the same as using ATMs, other (smart)-card-based systems, cellular phones etc."
- "creation of new sensitivities; creation of new senses of entitlement"
- "Big Brother" – no longer will internal moral systems be necessary because external surveillance could provide it all."

## Substantiating the thesis: the "role explication" aspect (5)

- "Explication of hidden or repressed aspects of life, personality, identity"
- "e.g., change in awareness about roles; growing dependency of IMS (and therefore problems when IMS is not properly available)"
- "people may become more aware of their various fragmented selves"

- "The stability persons identity is very important to them. Giving a person ease in presenting pseudonyms may blur his/her sense of identity and integrity."
- "People will develop higher awareness of the importance of their partial identities. Unfortunately, we have a chicken-and-egg-problem here: This is not only a likely consequence, but also a prerequisite for the adaptation of IMS."
- "You have to handle all your identities explicitly."

Misc. (6)

- "Control"
- "I don't know"
- "Mistaken identity"
- "Trust and safety"
- "I guess there will be, however I have no idea what it will be"

**Table 79: V46 – IMS – Improve or Worsen – Liability**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Worsen	8	9.0	9.6	9.6
	No change	23	25.8	27.7	37.3
	Improve	32	36.0	38.6	75.9
	I don't know	20	22.5	24.1	100.0
	Total	83	93.3	100.0	
	Missing	8	6	6.7	
Total		89	100.0		

**Table 80: V47 – IMS Improve or Worsen – Crime Prosecution**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Worsen	9	10.1	10.7	10.7
	No change	33	37.1	39.3	50.0
	Improve	23	25.8	27.4	77.4
	I don't know	19	21.3	22.6	100.0
	Total	84	94.4	100.0	
	Missing	8	5	5.6	
Total		89	100.0		

**Table 81: V48 – IMS Improve or Worsen – Clarification of Facts**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Worsen	9	10.1	10.7	10.7
	No change	17	19.1	20.2	31.0
	Improve	36	40.4	42.9	73.8
	I don't know	22	24.7	26.2	100.0
	Total	84	94.4	100.0	
	Missing	8	5	5.6	
Total		89	100.0		

**Table 82: V49 – IMS Improve or Worsen – Value of Admissible Evidence**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Worsen	9	10.1	10.6	10.6
	No change	23	25.8	27.1	37.6
	Improve	26	29.2	30.6	68.2
	I don't know	27	30.3	31.8	100.0
	Total	85	95.5	100.0	
	Missing	8	4	4.5	
Total		89	100.0		

**Table 83: V50 – IMS Improve or Worsen – Other**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Other categories	4	4.5	33.3	33.3
	Answer depends on the implementation of IMS	6	6.7	50.0	83.3
	No change	1	1.1	8.3	91.7
	IMS is only part of the picture	1	1.1	8.3	100.0
	Total	12	13.5	100.0	
	Missing	8	77	86.5	
Total		89	100.0		

Other categories (1)

- "Prevention of privacy violations (if an IMS is properly developed)"
- "computer search (Rasterfahndung)"
- "Ability to effectively implement mechanisms of centralised social control"
- "Privacy"

Answer depends on the implementation of IMS (2)

- "Sorry, no category, just an observation concerning V46-V49: Answers there will all depend on how an IMS will be implemented. So the correct answers would have been 'it depends...'"
- "it totally depends on the details of the IMS, no general answer possible"
- "not an extra category but a qualification – answers to above section very much depend on the type of IMS used for each type of application. Answers above predicated on appropriate use."
- "Can't answer any of 46-49, depends on system"
- "all the questions above: depend on actual implementation"
- "All of these are possible, but will depend on the policy decisions made about access to the IMS information, and how that information is stored, aggregated, and how long it is kept. This will be a basic tension between privacy advocates and government, at least within the US."

No change (3)

- "cannot be answered -- if the IMS and its legal context are properly designed, there should be no difference"

IMS is only part of the picture (4)

- "An IMS is only part of the picture. The questions above beg the question: 'If a given IMS were implemented, would it be possible to use it to enforce related laws...?' An IMS cannot fix any of these law enforcement problems without significant other administrative, procedural, legal and social changes."

**Table 84: V51 – IMS Improve or Worsen – Specified Other**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Worsen	4	4.5	40.0	40.0
	No change	1	1.1	10.0	50.0
	Improve	2	2.2	20.0	70.0
	I don't know	3	3.4	30.0	100.0
	Total	10	11.2	100.0	
	Missing	8	79	88.8	
Total		89	100.0		

**Table 85: V52 – IMS – Bottleneck**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bad usability	48	53.9	60.0	60.0
	Insufficient technol. development	20	22.5	25.0	85.0
	Insufficient security	7	7.9	8.8	93.8
	Insufficient privacy protection	3	3.4	3.8	97.5
	Too strong law enforcement	2	2.2	2.5	100.0
	Total	80	89.9	100.0	
Missing		8	9	10.1	
	Total	89	100.0		

**Table 86: V53 – IMS – Bottleneck, Other**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	User oriented	2	2.2	11.1	11.1
	Society oriented	10	11.2	55.6	66.7
	Technology oriented	3	3.4	16.7	83.3
	Misc.	3	3.4	16.7	
	Total	18	20.2	100.0	
Missing		8	71	79.8	
	Total		89	100.0	

User oriented (1)

- "poor interest by the users"
- "If you think of user-side technology: insufficient market demand by end users to start introduction from that side (...)"

Society oriented (2)

- "insufficient experience with computer/internet technology in the society"
- "insufficient knowledge for the need of it"
- "costs related to launching nation wide IMS"
- "Lack of standards"
- "too strong interests in non-privacy by government / intelligence / marketing industry"
- "(i)The risk of legislative initiatives which would negatively impact the mass deployment of IMS;
- (ii) (UK) Public antipathy towards anything which looks like an Identity Card.
- (iii) Existing investment in closed/proprietary authentication systems"
- "Level of trust in both the technology and the institutions responsible for the use of the technology."
- "Priority of IMS in the corporate IT agenda"
- "Lesser incentives for those able to widely deploy and cause adoption."
- "lack of consensus about what IMS should be/look like; therefore slow adoption / slow standardisation"
- "LACK OF AWARENESS FOR NEED AND ADVANTAGES IN CASE OF A USE AMONG THE SOCIETY"

Technology oriented (3)

- "insufficient pda/ clients"
- "insufficient interoperability/scalability"
- "ineffectiveness due to location tracking and ubiquitous computing with biometric identification"
- "(...) lack of compatibility with enterprise single sign-on solutions."
- "bad interoperability"

Misc. (4)

- "Trust"
- "No reason would be the reason (i.e. The bottleneck is the fact that no one is sure about what is the bottleneck)."
- "When you are dealing with a DB of 10s-100s of millions of entries, you can't assume it's perfect. As long as proponents claim that it's perfect, there will be too many flaws and horror stories."

**Table 87: V54 – Visionary IMS Texts**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	39	43.8	100.0	100.0
Missing	8	50	56.2		
	Total	89	100.0		

- "Abe Abelson MIT"
- "Carl Ellison on Electronic Identities: C.M. Ellison: What do you need to know about net people?"  
<http://world.std.com/~cme/html/congress1.html>"
- "Chaum 1985"
- "Chaum 81"
- "Chaum's 1985 paper in CACM, for what one can do technically. Microsoft's Passport documentation for what might actually happen."
- "Church Committee Report detailing US domestic political surveillance, David Chaum's ground breaking work on anonymous communications and credentials, Andreas Pfitzmann's work on implementing efficient anonymous communications"
- "David Chaum. Security without Identification: Transaction Systems to make Big Brother Obsolete. Communications of the ACM, 28(10):1030-1044,October 1985.Henk van Rossum, Huib Gardeniers, and John Borking et. al. Privacy-Enhancing Technologies: The Path to Anonymity, August 1995. Uwe Jendricke. Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement. Rhombos-Verlag. January 2003."
- "David Chaum: Security without Identification – Card Computers to make Big Brother Obsolete, Communications of the ACM 28/10 (1985) 1030-1044 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen, Karlsruhe, 1990 Michael McCandless: Managing your privacy in an on-line world, IEEE Expert 1997 January/February, p. 76-77"
- "David Chaum: Security Without Identification: Card Computers to Make Big Brother Obsolete; ursprüngliche Version: Security Without Identification: Transaction Systems to Make Big Brother Obsolete; Communications of the ACM, Vol. 28 No. 10, October 1985; 1030-1044Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity (PS); IBM Research

- Report RZ 3232 (#93278) 05/22/00 Computer Science/Mathematics; IBM Research Division; Zurich, May 2000"
- "Enriching Access Control to Support Credential-Based Specifications Pierangela Samarati"
  - "e-services, bank-services, mobile-e-services"
  - "EU Article 29 Data Protection Working Party 5063/00/EN/Final WP37"
  - "Hansen"
  - "Hansen/Köhntopp; Rost"
  - "<http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html>; <http://guir.berkeley.edu/privacyworkshop2002/papers/report.pdf>; <http://www.credentica.com/technology/book.html>"
  - "<http://www.dss.state.ct.us/digital/tomko.htm>; <http://www.inf.ethz.ch/vs/publ/slides/troubpatr.pdf>; <http://www.koehntopp.de/marit/pub/idmanage/index.html>"
  - "I am not conversant with the literature. My answers here are based on my projection of what IMS could mean."
  - "I am out of the office and cannot access references. Without access to references I can mention the seminal work by Chaum."
  - "I do not know."
  - "I don't know for IMS specifically, in general for the theoretical background it are still the texts of Chaum, for transfer into practical applications the texts on identity protector resulting from the Dutch/Canadian collaboration"
  - "I recommend the Liberty Alliances White Papers at [www.projectliberty.org](http://www.projectliberty.org)"
  - "Jendricke and Gerd tom Markotten 2000, Clauß and Köhntopp (Hansen) 2001, Berthold and Köhntopp (Hansen) 2001"
  - "John Borking, David Chaum, Andreas Pfizmann"
  - "Misc. papers by Stefan Brands, esp. introductory chapter of "Rethinking PKI..." book Peter Wayner – Translucent Databases" (2002) – very accessible survey of techniques for programmers"
  - "None that I would recommend to anyone"
  - "O. Berthold, M. Köhntopp, "Identity Management Based on P3P", Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, ICSI, Berkley, California, July 25-26, 2000, Springer LNCS 2009. Sebastian Clauß, Marit Köhntopp: Identity Managements and Its Support of Multilateral Security; in: Computer Networks 37 (2001), Special Issue on Electronic Business Systems; Elsevier, North-Holland 2001; 205-219"
  - "provide best security, personal data protection and usability"
  - "RAPID roadmap (<http://www.ra-pid.org>)"
  - "see RAPID report; IMS is the enabler of web services"
  - "1. The law alone can't protect privacy. 2. Not law but technology will protect privacy."
  - "Which will be visionary will depend very much on what the outcome of the technology and policy debates are"
  - "work of David Chaum, John Borking et al."
  - "[www.ipc.on.ca/scripts/index\\_.asp?action=3D31&P\\_ID=3D11361&N\\_ID=3D1=&PT\\_ID=3D11351&U\\_ID=3D0](http://www.ipc.on.ca/scripts/index_.asp?action=3D31&P_ID=3D11361&N_ID=3D1=&PT_ID=3D11351&U_ID=3D0); see also the references in [www.privacy.gov.au/news/speeches/sp104notes.pdf](http://www.privacy.gov.au/news/speeches/sp104notes.pdf); for a challenging time, visit Roger Clarke's web site – even if you disagree with him, the visit forces you to justify your position; start at [www.anu.edu.au/people/Roger.Clarke/DV/NotesCFP02.html#Bio m](http://www.anu.edu.au/people/Roger.Clarke/DV/NotesCFP02.html#Bio m); for an alternative point of view, see the views of Carol Coyne Benson as per the attached .pdf file"

**Table 88: V55 – Published IMS Texts**

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 0	38	42.7	100.0	100.0
Missing 8	51	57.3		
Total	89	100.0		

- "@inproceedings{ privacy:wspdrm01, title = "Privacy Engineering in Digital Rights Management Systems" author = "Joan Feigenbaum and Michael J. Freedman and Tomas Sander and Adam booktitle = "Proceedings of the {ACM} {W}orkshop in {S}ecurity and {P}rivacy in {D}igital {R}ights {M}anagement", address = "Philadelphia, PA", month = "November", year = "2001" }"
- "30. Tätigkeitsbericht, Ziff. 6.2"
- "Andrei Serjantov, George Danezis: Towards an Information Theoretic Metric for Anonymity. Privacy Enhancing Technologies 2002. Award at PET2003"
- "articles on my web page garymarx.net touch this especially on fraudulent identity, and on anonymity"
- "Birgit Pfizmann, Michael Waidner, Andreas Pfizmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen Datenschutz und Datensicherung DUD 14/5-6 (1990) 243-253, 305-315. (English translation: IBM Research Report RZ 3232 (#93278) 05/22/00,<http://www.semper.org/sirene/publ/PWP=5F00anoEcommerce.ps.gz>)"
- "Birgit Pfizmann, Michael Waidner: Privacy in Browser-Based Attribute Exchange; ACM Workshop on Privacy in the Electronic Society (WPES), Washington, Nov. 2002, to appear. Personal copy: <http://www.zurich.ibm.com/security/publications/2002/PfiWai2002bBBAE-privac=y-WPES.pdf>"
- "CCTV for Inside Your Head" 2001 – <http://www.law.duke.edu/journals/dltr/Articles/2002DLTR0005.html>" Cryptography and Democracy: Dilemmas of Freedom" in Liberty eds., Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet, London: Pluto Press, 1999, 81-125. BY Caspar Bowden, Foundation for Information Policy Research & Yaman Akdeniz, CyberLaw Research Unit, Centre for Criminal Justice Studies, University of Leeds = <http://www.cyber-rights.org/reports/yacb.pdf>"
- "Clauß/Pfizmann/Hansen/Van Herreweghen 2002; Köhntopp/Pfizmann in it+ti 2001; Hansen 2003 in Bäumler/Mutius 2003"
- "DRIM, <http://drim.inf.tu-dresden.de>"
- "E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, "Managing and Sharing Servents Reputations in P2P Systems," in IEEE Transactions on Knowledge and Data Engineering"
- "Fink, J. and A. Kobsa (2000): A Review and Analysis of Commercial User Modeling Servers for Personalization on the World Wide Web. User Modeling and User-Adapted Interaction 10(3-4), Special Issue on Deployed User Modeling, 209-249. <http://www.ics.uci.edu/~kobsa/papers/2000-UMUAI-kobsa.pdf>"
- "Fink, J. and A. Kobsa (2002): User Modeling in Personalized City Tours. Artificial Intelligence Review 18(1), 33-74. <http://www.ics.uci.edu/~kobsa/papers/2002-AIR-kobsa.pdf>"
- "G. Hogben, T. Jackson, M. Wilikens: A Fully Compliant Research Implementation of the P3P Standard for Privacy Protection: Experiences and Recommendations; European Symposium on Research in Computer Security 2002, Zurich 2002,

- 
- Springer LNCS 2502"
- "George Danezis: Mix-networks with Restricted Routes PET 2003."
  - "Hansen, Marit/Rost, Martin, 2002: Datenschutz durch computergestütztes Identitätsmanagement; in: Kubicek, Herbert(Hrsg.), 2002: Innovation@Infrastruktur (Jahrbuch Telekommunikation undGesellschaft, Band 10), Heidelberg: Hüthig-Verlag: 255-268."
  - "How to Protect Patients Rights to Medical Secret in Official Statistics, World Markets Research Centre Business Briefing: Global Infosecurity 2002; How to protect the rights of patients to medical secrecy in official statistics, Information Security Bulletin The International Journal for IT Security Professionals Volume 6, October 2001; Confidentiality and Data Protection – Patients Hospitalized in Switzerland, ISSE 2001, London Electronic proceedings, September 2001; How to protect patients rights, EEMA Briefing, Volume 14, no 3, September 2001."
  - "[http://2002.istevent.cec.eu.int/library/documents/living\\_with\\_security\\_engberg.pdf](http://2002.istevent.cec.eu.int/library/documents/living_with_security_engberg.pdf)  
<http://uir.berkeley.edu/privacyworkshop2002/papers/Privacy%20Authentication%20preliminay.PDF>"
  - "<http://cybersecurity.jrc.es>"
  - "[http://www.opengroup.org/dif/projects/im-scen/idmbs\\_1.pdf](http://www.opengroup.org/dif/projects/im-scen/idmbs_1.pdf)"
  - "<http://www.w3.org/P3P/>"
  - "J.J. Borking, C.D. Raab, Laws, PETs and Other Technologies For Privacy Protection – Journal of Information, Law and Technology (JILT) January 2001; Kenny S and Borking J, The Value of Privacy Engineering, Refereed Article, The Journal of Information, Law and Technology (JILT). 2002 (1) <http://elj.warwick.ac.uk/jilt/02-1/kenny.html>; G.W. van Blarkom, Guaranteeing requirements of data-protection legislation in a hospital information system with privacy-enhancing technology in The British Journal of healthcare Computing & Information Management – May 1998 Volume 15 Number 4 – Editor of: The impact of new technologies on privacy and data protection TILT, issue 15 (80 pages), March 2003 Authentication and/or identification through the virtual world Tilt, issue no 14, November 2002"
  - "JRC APPEL privacy preference interface."
  - "Kobsa (2001): Generic User Modeling Systems. User Modeling and User-Adapted Interaction 11(1-2), 49-63. <http://www.ics.uci.edu/~kobsa/papers/2001-UMUAI-kobsa.pdf>"
  - "Kobsa, A. and J. Fink (2003): Performance Evaluation of User Modeling Servers Under Real-World Workload Conditions. To appear in the proceedings of the 9th International Conference on User Modeling, Johnstown, PA. <http://www.ics.uci.edu/~kobsa/papers/2003-UM-kobsa.pdf>"
  - "Kobsa, A. and J. Schreck (2003): Privacy through Pseudonymity in User-Adaptive Systems. ACM Transactions on Internet Technology, 2003. <http://www.ics.uci.edu/~kobsa/papers/2003-TOIT-kobsa.pdf>"
  - "Mikael Nilsson, Helena Lindskog, Simone Fischer-Hübner, "Privacy Enhancements in the Mobile Internet", Proceedings of the IFIP WG 9.6/11.7 working conference on Security and Control of IT in Society, Bratislava, 15-16 June 2001."
  - "new ones at <http://www.zurich.ibm.com/security/identities/>"
  - "OECD is now making e-services survey about Finland, the survey is becoming ready in this summer, there is also text Finland citizen card, FINEID, and e-services"
  - "Oliver Berthold, Hannes Federrath: Identitätsmanagement; in: Helmut Bäumler (Hrsg.): E-Privacy, Vieweg, Wiesbaden, 2000. <http://page.inf.fu-berlin.de/~feder/publ/2000/BeFe2000IDMgmtSoAk/BeFe2000IDMgmt.html>"
  - "On a P3P user agent for the mobile Internet: Simone Fischer-Hübner, Mikael Nilsson, Helena Lindskog, "Self-Determination in the Mobile Internet", in: Proceedings of IFIP TC11 17th International Conference on Information Security (SEC 2002), Cairo/Egypt, 7-9 May 2002, Kluwer Academic Publishers."
  - "P. Bonatti, P. Samarati, "A Unified Framework for Regulating Access and Information Release on the Web," in Journal of Computer Security, 10(3), 2002."
  - "partly related: Cas, J., 2002, Privacy in Ubiquitous Computing Environments? 13th ITS European Regional Conference, Madrid, September 8-10"
  - "Richard Clayton, George Danezis, Markus G. Kuhn: Real World Patterns of Failure in Anonymity Systems. Information Hiding 2001: 230-244"
  - "Richard Clayton, George Danezis: Chaffinch: Confidentiality in the Face of Legal Threats. Information Hiding 2002: 70-86"
  - "Sebastian Claub, Marit Köhntopp: Identity Management and Its Support of Multilateral Security; in: Computer Networks 37 (2001), Special Issue on Electronic Business Systems; Elsevier, North-Holland 2001; 205-219"
  - "see PISA and RAPID reports"
  - "Uwe Jendricke and Daniela Gerd tom Markotten. Usability meets Security – The Identity-Manager as your Personal Security Assistant for theInternet. In Proceedings of the 16th Annual Computer Security Applications Conference, pages 344-353, December 2000. ISBN 0-7695-0859-6."
  - "Uwe Jendricke, Michael Kreutzer, and Alf Zugenmaier. Mobile Identity Management. Technical Report 178, Institut für Informatik, Universität Freiburg, October 2002. Workshop on Security in Ubiquitous Computing, UBICOMP 2002."
  - "Uwe Jendricke. Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement. Rhombos-Verlag, January 2003."
  - "[www.identitaetsmanagement.de](http://www.identitaetsmanagement.de); [www.datenschutzzentrum.de/idmanage](http://www.datenschutzzentrum.de/idmanage)"
  - "[www.netegrity.com](http://www.netegrity.com)"
  - "[www.privacy.gov.au/news/speeches/sp80.pdf](http://www.privacy.gov.au/news/speeches/sp80.pdf), [www.privacy.gov.au/news/speeches/sp104notes.pdf](http://www.privacy.gov.au/news/speeches/sp104notes.pdf),  
[www.privacy.gov.au/news/speeches/sp7\\_03.ppt](http://www.privacy.gov.au/news/speeches/sp7_03.ppt); [www.privacy.gov.au/news/speeches/sp92.ppt](http://www.privacy.gov.au/news/speeches/sp92.ppt)"
  - "Y. Deswarte, N. Abghour, V. Nicomette and D. Powell, "An Internet Authorization Scheme Using Smart Card-Based Security Kernels", in e-Smart 2001, (I. Attali and T. Jensen, Eds.), Cannes (France), Lecture Notes in Computer Science, 2140, pp. 71-82, 2001."
  - "Yves Deswarte, Noredine Abghour, Vincent Nicomette, David Powell, "An Intrusion-Tolerant Authorization Scheme for Internet Applications", in Sup. of the Proceedings of the 2002 International Conference on Dependable Systems and Networks (DSN2002), Washington, D.C. (USA), 23-26 juin 2002, pp."

**Table 89: V56 – Commentary**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Different theses	8	9.0	32.0	32.0
	Fair comments about lack of definition / description	5	5.6	20.0	52.0
	Fair comments about operational aspects of the questionnaire	6	6.7	24.0	76.0
	Statement: "I don't know much about IMS"	2	2.2	8.0	84.0
	Misc.	4	4.5	16.0	100.0
	Total	25	28.1	100.0	
	Total	8	64	71.9	
Missing					
Total		89	100.0		

## Different theses (1)

- "I see a typical chicken-and-egg problem: users won't use IMSs as long as there are only few applications that utilize them, and applications won't utilize IMSs as long as there are no users. Also, one has to set up an enormous security/privacy infrastructure if one wants to do it right. Who is going to pay for this?"
- "See RAPID report at www.ra-pid.org. Conclusion: Privacy Awareness is very low. Preventive privacy threat analysis (see www.pet-pisa.nl) is sine qua non in order to build safe IMS and must be part of legislation."
- "The principal problem seems to me that abuse of personal information cannot be traced to the responsible party and damaged one can hardly be repaired. This leads to a all-or-nothing concept of privacy: if a single one of the entities involved at any time leaks personal information, it is irreversible."
- "I think that the use of credentials in IMS will be vital."
- "Die Entwicklung geht voraussichtlich in Richtung von Zugriffsrechten der Staatsanwaltschaften. Trotz pseudonymisierter Nutzung sind deren Rechte gemäß §100a StPO zu gewährleisten. Der Schutz dürfte sich daher vor allem gegen Dritte und Adressaten (Betreiber von E-Commerce oder anderen Internetangeboten) richten."
- "IMS is a very important topic for corporations + government – it is more about getting their operations in order than about law enforcement however
- Companies + governments need to centralize their identity + access management as the number of applications + users increase dramatically. I can be reached at: \*@\*.com"
- "I attended the RSA Conference 2003 in San Francisco and found IMS was one of the two major topics there. However, the speakers only talked about the merits of integration and never touched on privacy protection by linkability. Probably, user controlled linkability of identity is not very popular in US, I am afraid."
- "I think that managing the public perception of identity and privacy will be defining issues of online interaction over the next 10 years in Western democracies."

## Fair comments about lack of definition / description (2)

- "The definition of an IMS is so unclear that several questions does not make sense – example 46-51."
- "IM NOT FAMILIAR WITH THE CONCEPT OF IMS. I NEED A MORE DETAILED DESCRIPTION OF WHAT THE SYSTEM WOULD BRING CONCRETELY IN MY DAILY LIVE AT WORK/HOME. HERE IS A CLEAR EXAMPLE OF THE GAP BETWEEN SPECIALIST AND NON (not yet) SPECIALIST. REGARDS"
- "I must admit I missed a precise definition or explanation of the term IMS. Therefore I was unable to match existing or possible applications with the questions above. The closest concept I am aware of is the Identity Protector."
- "I suspect IMS means many different things to different people, you should have made it more clear what sort of system should be thought about :)"
- "All answers depend finally on unspoken assumptions. The answers will change dramatically, if PKI and digital signatures come into the picture."

## Fair comments about operational aspects of the questionnaire (3)

- "This e-mail looks like spam, I already had my finger on the Delete key. You probably should use another sender name."
- "V46-V49: this really depends on the design"
- "I am afraid the questionnaire is misleading. 18 seconds per answer is appropriate for yes/no answers, but not for "suggest your own" ones. A better introduction about Identity Management Systems would be appropriate. Sometimes it is not clear what you mean. Question V39 is unclear. In fact, I still do not know what it means. So is V38. Does it mean "is it important that the government has control over Identity Management Systems?" (i.e., do you agree with the government having control ...) or does it mean "is the question of who has control over ... important to you"? V30 I do not consider that an important goal."
- "incomprehensible question on law enforcement"
- "aren't V38 and V39 the same question? also, V31 and followings are easy to misunderstand: should I state whether I think these things are important or not for a \_good\_ IMS or for a \_popular\_ IMS? these are two quite different things for me, but I tried to answer the first."
- "Nicht verstanden: 15, 16, 17, 18"

## Statement: "I don't know much about IMS" (4)

- "It's not clear to me that I'm the sort of person you wanted to be filling out this questionnaire. I really don't know much about IMS practices now"
- "I really don't know anything about IMS. Sorry I couldn't be of more help."

Misc. (5)

- "greetings and good luck in today's difficult environment"
- "good luck for the analysis"
- "Warum gibt es den Fragebogen auf Englisch und nicht (wenigstens auch) auf Deutsch?"
- "Please note that the 25th conference of data protection commissioners, to be held in Sydney 10-12 September 2003 will have sessions explicitly dealing with identity management issues. Working titles for Sessions include "Identity & Privacy: Who wants to know & why"; "Identity: Now you see it now you don't". Follow the Conference web site at [www.privacyconference2003.org](http://www.privacyconference2003.org)"

**Table 90: V57 – Answers**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely answered (without V54 to V56)	80	89.9	89.9	89.9
	Not completely answered	9	10.1	10.1	100.0
	Total	89	100.0	100.0	

**Table 91: V58 – Syntax**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Syntactically correct	70	78.7	78.7	78.7
	Syntactically wrong	19	21.3	21.3	100.0
	Total	89	100.0	100.0	

**Table 92: V59 – Reminder**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Before reminder	23	25.8	25.8	25.8
	After reminder	66	74.2	74.2	100.0
	Total	89	100.0	100.0	

## 1.3 Some Methodically Notes

The e-mails containing the questionnaires were sent on April 3, 2003, including the request to answer until April 9. On April 9, a reminder mail was sent. The questionnaires that had been filled-in and returned until May 2 were evaluated. Almost exactly 75 % of the answered questionnaires were only returned after the reminder of April 9, i.e., after the first dateline had expired.

### 1.3.1 Return Quota

**Table 93: Return Quota**

Total of experts addressed via e-mail:	n = 246
Undeliverable e-mails:	n = 8
Number of experts addressed effectively after error handling:	n = 238 (= 100 %)
Number of those who answered with a commentary but did not fill in the questionnaire:	n = 20
Number of those who answered the entire questionnaire:	n = 89
<b>Reaction quota</b> (reaction with and without answering the questionnaire):	45.80 %
<b>Effective return quota</b> of the usable questionnaires:	37.40 %

Among the 8 % of interviewees who reacted without answering the questionnaire, there were three typical reactions:

Most of those who reacted without answering the questionnaire felt not competent enough concerning the topic:

*"Unfortunately, I don't think I qualify as an expert on Identity Management Systems, and therefore I would have to decline from filling your questionnaire."*

Or: *"I don't think that I am an appropriate respondent to this questionnaire: I could not offer informed opinion on these questions. Sorry."*

Or: *"We have received your questionnaire, but there are still a few unclear issues. We have difficulty understanding what kind of "identity management" you refer to. Could you give me an example of the kind of system you mean (preferably with a hyperlink)?"*

Others pointed out that filling in such questionnaires takes too much time or that the dateline was too short:

*"I currently receive one to three requests to fill out surveys per week. Most are quite interesting, legitimate research projects. However, due to the volume of requests I receive, I am no longer able to answer any such requests. Sorry I can't be of more help."*

Or: *"While we are basically willing to co-operate with other data protection authorities, I personally think that the timeframe of less than one week for a seven page questionnaire with 56 entries is far too short. We do have other work. Why this extremely short deadline?"*

Third, there were profound statements in which the denial was justified in content:

*"Sorry, but I don't accept the perspective from which the questionnaire has been developed. And I find it difficult to explain through your questionnaire that I don't accept the \*concept\* of identity management, and that I don't think it has anything to do with Datenschutz, far less Personenschutz. It's purely an organisational device for further undermining personal self-determination. If that's any use to you, feel free to quote it."*

Or: *"Regarding the questionnaire, the questions are not so simple to answer. As a matter of facts it will take us a lot of time to answer them as on nearly all questions we would answer: 'it all depends' and then give lots of details i.e. questions 1, 3, 4, 5, 6, 7, 8, 10, 12, 13, 14. So please forgive us not to answer at this stage. Of course your questionnaire is very interesting as summing up many faces of the identity question. The more simple questions/answers are: question 9 ID card is not compulsory in France, other documents can prove identity where necessary. – question 11 France has adopted a comprehensive data protection law, did you not know?"*

### 1.3.2 Methodical Inadequacies and Mistakes

The variable V2 was badly specified because it was not clear enough if a workgroup, a department or an institute or the whole organisation was meant by the unit.

To the variable 30, the unit "years" would have had to be added. About a third of those who answered have entered a text instead of a number or estimated a time period. Several statements like the following were made: *"Not in the foreseeable future"*, *"Forever, unless government will enforce it"*, *"Few Years"*, *"I will not live to see a society-wide implementation translated to: 40 years (2 generations)"*, *"I don't think market forces will bring it about; there's too much overhead for anyone other than fanatics to use. Won't happen on a large scale unless regulation requires it or Microsoft implements it."*, *"less than 10 years for more than 50 %"*, *"forever"*, *"Maybe in 20 years but maybe never. Not in the short term and not until very serious privacy, abuses (well beyond identify theft) are observed."*, *"extremely unlikely, since proofs of compliance are hard."*, *"I don't think society wide-multi-purpose IMS is likely or desirable. We don't have all-use ID cards."*, *"I do not consider that an important goal."*, *"Impossible to realize."*, *"depends on several developments, don't know"*.

The variable V52 invited every second participant to enter multiple answers, i.e., unambiguous cross-tabling is impossible. However, it is made clear that 85 % of the interviewees consider "bad usability" and "insufficient technological development of a society-wide infrastructure for an IMS" as a "potential main bottleneck" concerning a mass distribution of an IMS.

---

Some users report that the questionnaire had been identified as spam either by the spam filter or after quickly browsing through of the new e-mails. "This e-mail looks like spam, I already had my finger on the Delete key. You probably should use another sender name."

### **1.3.3      Generally Remarks on the Questionnaire (V56)**

The following statements were made as general methodically-oriented, criticising remarks on the questionnaire (V56):

- "V46-V49: this really depends on the design",
- "I am afraid the questionnaire is misleading. 18 seconds per answer is appropriate for yes/no answers, but not for 'suggest your own' ones. A better introduction about Identity Management Systems would be appropriate. Sometimes it is not clear what you mean. Question V39 is unclear. In fact, I still do not know what it means. So is V38. Does it mean 'is it important that the government has control over Identity Management Systems?' (i.e., 'do you agree with the government having control ...') or does it mean 'is the question of who has control over ... important to you?' V30 I do not consider that an important goal."
- "incomprehensible question on law enforcement"
- "aren't V38 and V39 the same question? also, V31 and followings are easy to misunderstand: should i state whether i think these things are important or not for a \_good\_ IMS or for a \_popular\_ IMS? these are two quite different things for me, but i tried to answer the first."
- "Nicht verstanden: 15, 16, 17, 18"

## 2 RAPID'S ROADMAP ON PRIVACY AND IDENTITY MANAGEMENT

The RAPID project ("Roadmap for Advanced Research in Privacy and Identity Management") has been working since 2002 on developing a strategic roadmap for applied research in the area of privacy and identity management (PIM). The preliminary results are quoted here [Huizenga 2003]:

### 2.1 Introduction

*The strategic roadmap for applied research in the area of privacy and identity management, is developed based on the input of leading experts and stakeholders structured in two main streams consisting of five RTD roadmaps:*

#### Stream 1: **Socio-economic and legal RTD (SE-L Roadmap)**

R-SE: Research for Socio-economic aspects (new computing paradigms)

R-L: Research for Legal aspects

#### Stream 2: **Technology-Business RTD (TB-Roadmap)**

R-MDIM: Research for Multiple and dependable identity management

R-PE: Research for PET for Enterprise

R-PI: Research for PET in Infrastructure

The R&D model is used to allocate the most interesting research topics and their relation between the different phases of the implementation and the time frames.

The two phases used in the PIM roadmap are:

B = Business development and process/product development

T = Applied and fundamental technical research

The time frames used in the PIM roadmap are Short term (0-3 years), Mid term (3-5 years) and Long term (5-10 years). The priorities used are Essential (E), Important (I) and Nice to have. To structure all the R&D-items from the technology topics in clusters, we focus on the parts marked as Essential and Important R&D. This is an iterative process, based on the visions of business models for PIM, which has to develop according the time scales and different phases in an integrated way.

### 2.2 Research Plan PET in Enterprise (R-PE)

**Table 94: Research Cluster PET in Enterprise**

	Research Cluster PET in Enterprise	Imp	S (0-3)	M (3-5)	L (5-10)
R-PE-1	<b>Federated and End-to-End Identity Management Systems</b> <ul style="list-style-type: none"> <li>- Scalable IM systems with privacy aware access control and distributed Trust Management</li> <li>- End-user devices with privacy friendly access control based on user profiles and preferences</li> </ul>	E	T B-T  T	B T-B  B	T-B
R-PE-2	<b>PET Functions (Anonymity and Data Minimisation/Protection)</b> <ul style="list-style-type: none"> <li>- Privacy friendly access control</li> <li>- Anonymous credentials</li> <li>- Anonymity in data (files, databases)</li> <li>- Business and personal data analysers</li> <li>- Audit functions and tools</li> </ul>	E  I  I  I	T  T  T  T-B	T-B  T-B  T-B  T-B	T-B  T-B

<b>R-PE-3</b>	<b>Identity Management Ontology and Policies</b> - Identity management ontology and data protection ontology development - Composition and refinement - Tools to create preferences (languages) - User choice - Policies supporting user IM	E E E I I	T T T T T	T-B T-B T-B	T-B
<b>R-PE-4</b>	<b>Enforcement</b> - Enforcement architecture - Advances in cryptography and application methods	I		T	T-B
<b>R-PE-5</b>	<b>Validation services</b> - Evaluation tools - Self-certifying compliance - Voluntary reporting system - Testing and verification	I		T	T-B

The PET in Enterprise research plan (R-PE) is based on two main topics, which are **essential** and have to be done first **in short term**:

- **R-PE-1:** The product development combined with technological implementation of scalable IM systems, including distributed Trust Management, and the technological development of end user IM devices, which can be integrated with the scalable IM systems.
- **R-PE-2:** The fundamental research of standard PET-functions for anonymity/pseudonymity in privacy friendly access control.
- **R-PE-3:** The fundamental research for Identity Management Ontology and Policies with generic models, categorisation and composition and refinement.

**Important PE-research topics for the short term** are:

- **R-PE-2:** The fundamental research of anonymous credentials and anonymity in files and databases.
- **R-PE-3:** The fundamental research of tools for Identity Management and Data Protection Ontology, Composition and refinement, User policies and preferences, User choice, Preference language and Policies supporting user IM.

In the R-PE plan, prototyping and business development of the scalable IM-systems and IM-User devices will be continued in the medium term period (3-5 year).

**Essential research PE-topics for the medium term** are:

- **R-PE-2:** Transfer of the fundamental research in applied research and prototyping for privacy friendly access control, combined with product/process and business development.
- **R-PE-3:** Transfer of the fundamental research in applied and business development for anonymity in files and databases.

**Important PE-topics for the medium term** are:

- **R-PE-2:** Applied Research and prototyping for Tools for Business and personal data analysers and Audit functions.
- **R-PE-3:** Fundamental, applied research and prototyping for quality assurance as risk analysis and privacy threat analysis, validation services, evaluation tools, testing and verification methods and techniques.
- **R-PE-5:** Fundamental, applied research and prototyping of enforcement architecture and advances in cryptography and application methods.

## 2.3 Research Plan PET in Infrastructure (R-PI)

**Table 95: Research Cluster PET in Infrastructure**

	Research Cluster PET in Infrastructure	Imp	S (0-3)	M (3-5)	L (5-10)
R-PI-1	<b>Infrastructure Privacy</b> <ul style="list-style-type: none"> <li>- Address privacy: mixes, dynamic addresses, ad hoc networking</li> <li>- Location privacy: mobile operators, location services, pervasive computing</li> <li>- Service access privacy: anonymity proxy, e-mail pseudonyms, multiple identities, policy negotiation</li> </ul>	E E E	T T T-B	B B	B
R-PI-2	<b>PET Functions (Anonymity and Data Minimisation/Protection)</b> <ul style="list-style-type: none"> <li>- Privacy friendly access control</li> <li>- Trust in pseudonym authenticity</li> <li>- Feedback channel</li> <li>- Anonymous credentials</li> <li>- Anonymous communication</li> <li>- Self termination anonymity specific identity completion</li> <li>- Privacy enhanced data mining/warehouse</li> <li>- Anonymity in data (files, databases, etc.)</li> <li>- Audit functions and tools</li> </ul>	I E E E I I I	T T-B T-B T-B T T-B T	T-B T T-B T-B T-B T-B B	T-B
R-PI-3	<b>Identity Management Ontology and Policies</b> <ul style="list-style-type: none"> <li>- Identity management ontology and data protection ontology development</li> <li>- Composition and refinement</li> <li>- Tools to create preferences (language)</li> <li>- User choice</li> <li>- Policies supporting user IM</li> </ul>	I I I I I	T-B T-B T-B T-B B	T-B T-B T-B T-B B	B B
R-PI-4	<b>Enforcement</b> <ul style="list-style-type: none"> <li>- Enforcement architecture</li> <li>- Violation detection, control of damage/logging</li> </ul>	E I	T	T-B T-B	B
R-PI-5	<b>Validation services</b> <ul style="list-style-type: none"> <li>- Evaluation tools</li> <li>- Self-certifying compliance</li> <li>- Voluntary reporting system</li> <li>- Testing and verification</li> </ul>	I I I I		T T T T	B B

## 2.4 Research Plan Multiple and Dependable Identity Management (R-MIM)

**Table 96: Research Cluster Multiple and Dependable Identity Management**

	Research Cluster MIM	Imp	S (0-3)	M (3-5)	L (5-10)
R-MIM-1	<b>Identities Life Cycle Management, Administration for Multiple Identities' management</b> <ul style="list-style-type: none"> <li>- Provisioning, revocation, profile management, prevention of identity proliferation.</li> <li>- Development of user-side architecture</li> <li>- Personal mobile IM devices and media</li> <li>- Distributed registration/cert. authorities</li> <li>- Integration with other services</li> </ul>	E	T	T-B	T-B
R-MIM-2	<b>PET Functions (Anonymity, Dependability and Trust Management)</b> <ul style="list-style-type: none"> <li>- Anonymity support</li> <li>- Dependability and accountability</li> <li>- Theft and unauthorised transfer prevention</li> <li>- Custom encryption techniques</li> <li>- Control on SSO identity disclosure</li> <li>- Trust models and support of trust levels</li> </ul>	I E	T T-B	T-B	T-B

R-MIM-3	<b>Ontology and Digital Identities Representation</b> - Identity ontology - Identity syntax - Identity interoperability and portability - Identity extensibility	I	T	T	B
R-MIM-4	<b>Cross-Domain Identity Communication</b> - Federated identity management support - Distributed management of user profiles - Distributed update support	I	T	T-B	T-B
R-MIM-5	<b>Controlled Dissemination of Authenticated Information</b> - Privacy and secondary use control - Negotiation protocols - Linkability - Owners accountability	I	T-B	T-B	T-B

## 2.5 Research Plan Socio-Economic (R-SE)

Table 97: Research Cluster Socio-Economic PIM

	Research Clusters Socio-Economic PIM	Imp	S (0-3)	M (3-5)	L (5-10)
R-SE-1	<b>Privacy Experience and Classification in Europe for the Citizen</b> - Privacy experiences of citizens in European countries with regard to different ICT - Privacy experiences of different people in their interactions with new ICT - What, when and why trust for citizens in different (ICT-facilitated) relationships with different parties and of how PIM can be effective - Local cultural differences in Europe (north, south, east, west) of citizens' perceptions and practices of privacy and data protection arrangements - Let citizens have (more) control over their personal data	E	P P	B B	B
R-SE-2	<b>Analysis of the PIM Relation for the Digital Identity Services (Public IM Service)</b> - Classification of electronic public services in EU and appropriate minimal security levels - Conditions for reliable digital IM systems in EU - Appropriate levels of identification for different policy cases within European countries - Standards for privacy and identity management regarding the use of ICT	E	B P	B P	B
R-SE-3	<b>Analysis of the PIM Relation for the Government to Citizens and Enterprises</b> - Local cultural differences for privacy and identity management for member states and at the EU - Trust, transparency and risk in information relationships between government and citizens - Conditions for a holistic approach of privacy issues for governments - Privacy protection and combating crime and terrorism	I	P B	B	B
R-SE-4	<b>Analysis of the Ways and Conditions to Raise Awareness of ICT Users</b> - Development of PIM education and pr-plan - Transparency promotion to citizens with regard to the collection and use of personal data	I	B	B	
R-SE-5	<b>Analysis of the Ways and Conditions to Stimulate PIM Producers and Development of PIM Business Models</b> - In an early stage of the design process pay attention to privacy and identity management issues - Economic incentives and hindrances to protect and to disclose personal information on the consumers' level as well as on the companies' level - Economic incentives and hindrances of companies and consumers to adopt or to refuse PETs	I	P B B		

	<ul style="list-style-type: none"> <li>- Companies' costs and benefits aligned with the adoption or decline of PETs</li> <li>- Volume, cost, value and benefits of personal information collected in Internet transactions between vendors and consumers</li> <li>- Context- and market-related categorisation of the strategic value of personal information</li> <li>- Economic incentives for PETs and for improved regulation of privacy protection</li> </ul>		B B B B	B B B B
--	--	--	------------------	------------------

## 2.6 Research Plan Legal (R-L)

**Table 98: Research Cluster Legal Aspects PIM**

	Research Clusters Legal aspects PIM	Imp	S (0-3)	M (3-5)	L (5-10)
R-L-1	<b>Law and Regulation</b> <ul style="list-style-type: none"> <li>- Communication</li> <li>- Compliance</li> <li>- Enforcement mechanisms and the role of supervisors</li> </ul>	I	B B	B B	B P
R-L-2	<b>Law and Technology</b> <ul style="list-style-type: none"> <li>- Ontologies: applying the European regulatory framework (particularly Directives 95/46/EC and 02/58/EC) to the new technological environment</li> <li>- Monitoring privacy decreasing technologies and the privacy protection of vulnerable categories of individuals in society</li> <li>- Concepts of legitimated use of anonymity and pseudonymity, and their restrictions</li> <li>- Legal implications of enhancing protection of privacy in potential privacy decreasing technologies (e.g., PKI + DRM)?</li> <li>- Prevention of privacy decreasing application fields (e.g., e-government and privacy + law enforcement and privacy) and how can we intercept them timely?</li> </ul>	I	P P P B	P P	P B
R-L-3	<b>Privacy and IM Technology Law</b> <ul style="list-style-type: none"> <li>- Amount of identification needed for each particular environment?</li> <li>- Rules for privacy protection service providers?</li> <li>- Individual freedom to use privacy enhancing technologies?</li> <li>- Legal implications of (multiple) on-line identities</li> <li>- Rules for identity managers</li> <li>- Control instruments for identity holders</li> </ul>	E	B P B P P	B P P	B P P

## 2.7 Overall Roadmap

This Chapter describes the overall roadmap. The overall roadmap is derived from the individual roadmaps from the streams, and reflects all the essential research topics that the streams have in common. As can be seen in Table 100 research topics that start out as fundamental research will eventually lead to business development topics. This path of growth is needed to make sure in the future research funds will be well spent. The roadmaps for the three-technology areas are combined in one Table 99 to look for integration of the essentials parts for the overall roadmap.

**Table 99: Selection of the Essential and Important Technology Business RTD for PIM**

Time	B/ T	Research Plan <b>MIM</b>	Research Plan <b>Infrastructure</b>	Research Plan <b>Enterprise</b>
Short		- User PIM service (theft)	PIM service (access)	- PIM service (B.Model)
Short	T	- User PIM (life cycle, theft) - Ontology + representation	- Infrastructure PIM (address) - Ontology + policies - PET functions - Enforcement architecture	- Scalable PIM systems - PIM user devices - Ontology + policies - PET functions
	B	- Ontology representation - User PIM - Controlled dissemination	- Ontology + policies - Infrastructure PIM (address, location) - Enforcement	- Ontology + policies
Mid	T	- PET functions - Ontology representation - User PIM - Controlled dissemination	- PET functions - Ontology + policies	- Scalable PIM systems - Ontology + policies - PIM user devices - Enforcement - Validation
Long	B	- Ontology representation - Cross domain IM - User PIM	- Ontology + policies - Enforcement	- Ontology + policies - Enforcement - Federated PIM systems - Privacy access control
Long	T	- PIM Cross-domain	- PET functions - Enforcement	- Federated PIM systems - Enforcement - Validation

B = Business development and process/product development

T = Applied and fundamental technical research

Table 100: RAPID Roadmap

	Short-term (0-3 years)	Mid-term (3-5 years)	Long-term (5-10 years)
Business Development	R-PI-1 PIM service (Access)		
		R-PI-3/R-PE-3 Ontology + policies	
	R-PE-1 PIM service (B. Model)		R-PE-1 Federated PIM systems
	R-SE-1 Privacy experience & classification EC		
	R-SE-2 Classification and Conditions PIM services EC		
		R-SE-3 PIM and Government	
		R-SE-4 PIM and producers + R-SE-5 business models	
		R-L-1 Law and Regulation	
		R-MIM-1 User PIM	
		R-MIM-3 Ontology + representation	
Business Process/ Product Innovation	R-PE-1 Scalable PIM systems and user devices		
		R-L-3 Privacy and IM Technology Law	
		R-PE-4/R-PI-4 Enforcement	
	R-MIM-5 Controlled dissemination		R-MIM-4 Cross Domain IM
	R-PI-1 Infra PIM (Addr. Location)		
		R-PE-2 Privacy Access Control	
		R-L-2 Law and Technology	
	R-PI-2 PET functions		
		R-MIM-4 Cross Domain IM	
	R-MIM-5 Controlled dissemination		
Technology		R-PE-4/R-PI-4 Enforcement	
		R-PE-1 Federated PIM systems	
		R-PE-5 Validation	
	R-MIM-3 Ontology + representation		
	R-PE-3/R-PI-3 Ontology + policies		
Fundamental Research	R-PI-1 Infra PIM (Addr. Location)		
	R-PI-4 Enforcement Architecture		
	R-MIM-1 User PIM		
	R-PE-2 PET functions		R-PE-5 Validation

 = essential = important

### 3 ARTICLE 29 WORKING PARTY COMPARISON

The following excerpt is taken from [Art. 29 DPWP 2003]:

**Table 101: Comparison of the Presently Existing On-line Authentication Systems**

Mozilla Password Manager	Authentication by Proxy	Microsoft Passport	Liberty Alliance
No third party identity provider	Third party identity provider chosen by the end user	Microsoft as third party identity provider	Third party identity provider chosen by the service provider (mutual contracts)
Access via own PC only	Access via the channels offered by the authentication provider	Possible access via different devices, currently mainly PC-like	Possible access via different devices, among which mobile phones
Currently available and widely used	Limited availability	Currently available and used by all Microsoft services	First implementation stages
User ID and password per site	User ID and password per site	Single user ID and password	Password and user ID per site
User is identified with user ID and password	User is identified with user ID and password	Single unique identifier for a user (PUID)	Different handle per pair of sites
No contract needed	Contract between end user and provider	Contract between Microsoft and service provider	Contract between every site in a circle of trust
-	Authentication protocol requires proxy provider to know which sites with authentication are visited (storage of UID/password combination per site)	Microsoft uses a unique PUID per user	Unique handle per user per federated pair of site. Authentication provider needs to know only sites where the identity is federated
Using different user ID's, end user can prevent service providers from combining data among themselves	Using different user ID's, end user can prevent service providers from combining data among themselves	Unique PUID identifies the user. Contractual agreements prevent service providers to combine their data	Data on users can be combined by pairs of sites only. Sites determine their own mutual contracts
Service provider is the only data controller	Both service provider and proxy provider are data controller	Service provider dealing with authentication requests and Microsoft are data controller	Service providers within a circle of trust become data controllers at the time users visit their sites
No data transfer between controllers	Authentication information is passed between controllers	Authentication and in some cases profiling information is passed between controllers	Authentication information is passed between controllers
User controls all communication	User consent needed	User consent needed (required by Microsoft's implementation and contracts)	Normally, user consent is needed twice per federation, but automatic federation is possible
Authentication protocol does not require cookies	Authentication protocol does not require cookies	Current implementation uses cookies	Current implementation uses cookies

## 4 LEGAL MATERIAL

### 4.1 Electronic Signature

In principle, normal business regulations are valid concerning the Internet and electronic transactions. Contracts resulting in a binding obligation for all parties can be made by e-mail or a simple click. To ensure authenticity and have potential evidence in front of court in an anonymous environment, the use of electronic signatures is reasonable. Additionally authenticity can be gained by using pseudonyms, a possibility the legal systems of some countries provide (e.g., Germany, § 5 paragraph 3 Signaturgesetz).

The term "electronic signature" among other things belongs to the European Signature Directive that should be more open to all kinds of signature technologies than the technologically defined term "digital signature".

#### 4.1.1 Types of the Electronic Signature in Comprehensive Law (Europe)

Germany was one of the first countries of the world with a law regulating digital signatures. The "Signaturgesetz" (SigG) became effective on 01.11.1997. By the signature law and the ordinance "Signaturverordnung" the legal framework conditions of the construction of signatures and the certification by trust centres were regulated [cf. Schicker 2002 ]. At first it was refrained to release further-reaching right effects connected with the application of digital signatures. It was wanted to first gain experience with this new technology.

Until now, further countries of the EU developed their own regulations regarding digital signatures. To avoid different regulations within member states the EU approved Directive 1999/93/EC of 13.12.1999 on a Community framework for electronic signatures (Official Journal L13 of 19.01.2000, p. 12). Furthermore this also contained a graded system of different kinds of signature regulations regarding legal effectiveness and ability of proof. The EU-Directive is neutral concerning technology and implementation and changes nothing on party autonomy or contractual freedom.

The following exemplarily depicts the implementation of the directive as it was realised in Germany.

##### 4.1.1.1 Other Electronic Signatures

In principle according to § 1 paragraph 2 SigG signature methods not fulfilling the requirements of the SigG are also allowed. The use of signature methods like PGP or complete free systems therefore is also permitted. The legal validity remains restricted to areas in which the law doesn't require particular form.

##### 4.1.1.2 Advanced Electronic Signatures

Prerequisites for the advanced electronic signature are:

- exclusive assignment of a signature to the signature key owner (§ 2 no. 2 a) SigG)
- identifiability of the signature key owner (§ 2 no. 2 b) SigG)
- the signature must be created with resources, that the signature key owner can hold under his exclusive control (§ 2 no. 2 c) SigG)
- any subsequent alteration of the data must be recognisable (§ 2 no. 2 d) SigG).

---

#### **4.1.1.3        Qualified Electronic Signatures**

For qualified electronic signatures according to § 4 SigG the obligation of §§ 5 -14 SigG must be met. For this it is sufficient that the provider announces the start of the service at the German "Regulierungsbehörde für Telekommunikation und Post" (RegTP) [Roßnagel 2002]. A voluntary accreditation is not necessary.

The following points additionally join the prerequisites of the advanced signature:

- the signature must have been created using a safe signature construction unity (§ 2 no. 3 b) SigG)
- the signature must be based on a valid qualified certificate at the time of its production (§ 2 no. 3 a) SigG).

Qualified electronic signatures of providers from within the EU must be treated as equivalent to German signatures if they correspond to at least the minimum requirements provided in the EU signature directive. For example, the EU signature guideline does not dictate the regulation of a preservation period as it applies to the German law (cf. Annex II lit. i) SigRL). The German law regulates a preservation period of five years in § 4 SigV.

#### **4.1.1.4        Qualified Electronic Signatures based on voluntary Accreditation (Accredited Electronic Signature)**

The accredited electronic signature is regulated in § 15 SigG and goes beyond the standard regulations of the EU directive. So not only the obligations of the §§ 5-14 SigG have to be met as in case of the qualified electronic signature. The supplier must in particular prove this by an initial examination / voluntary accreditation. An re-examination is carried out every three years at the latest (cf. § 11 paragraph 2 SigV).

An equality of foreign signatures is realised only when proof of equal safety is furnished (cf. § 23 paragraph 2 SigG).

### **4.1.2        Legal Effects**

Not only the types of the signatures were regulated Europe-wide, the directive also instructed the member states to regulate the recognition of electronic signatures in their systems of laws for different legal transactions in civil and administration law. This also contained the modification of proof methods to give strong weapons into the hand of the users and acceptors of electronic signatures in a dispute in front of court.

The regulation shall exemplarily be depicted using the German law again.

#### **4.1.2.1        Other Electronic Signatures**

For other electronic signatures there are no particular regulations for a legal effect. They can be employed everywhere where the law does not require particular form. As in the case of verbal contracts and simple e-mails with corresponding contents a valid contract takes place according to German law.

#### **4.1.2.2        Advanced Electronic Signatures**

The advanced electronic signature obtains the same rules as the 'other electronic signatures'. It is also only applicable where the law does not stipulate particular form for correct business behaviour. By the increased prerequisites it can however be easier to prove the actual giving of the explanation.

#### **4.1.2.3 Qualified Electronic Signatures**

The application field for the qualified electronic signature was expanded in the German law by the §§ 126 pp. BGB. In most cases in which writing is demanded according to the law the "signature" also can be carried out with the qualified electronic signature (cf. § 126 paragraph 3 BGB). Only for particularly serious business the real writing or even stronger ways of form are still required such as at declarations of surety (§ 766 BGB), purchases of property or the erection of a will (§ 2247 BGB).

#### **4.1.2.4 Qualified Electronic Signatures based on voluntary Accreditation**

For the accredited electronic signature there is no extended application field in the business area. This was also already stipulated by the corresponding EU directive. Only in the area of administration the individual countries are allowed to also dictate stricter prerequisites than the one to the qualified electronic signature for certain actions. This can be, e.g., the accredited electronic signature in Germany. Reason for this potentially could be that accredited signatures had to remain testable for 30 years. According to German law the supplier of qualified signatures is obliged for only five years after the year the validity of the certificate has expired.

#### **4.1.3 Probative Value**

Who wants to sue for his right in front of court with digital signed documents must prove the substantiating facts. If he does not succeed, his complaint will be rejected. On the other side the one who wants to defend himself against a complaint must have counterevidence or show the insufficiency of the evidence of his opponent.

The possibilities for this are regulated very differently within the systems of laws in Europe and the world. For this German law shall exemplary be depicted once more.

In principle, the German right has different regulations for different kinds of evidence, that arrange how to prove something. Electronic documents such as e-mails according to § 371 paragraph 1 ZPO (German civil law) are seen as "objects of appearance" (Augenscheinobjekte). The judge is free at the assessment of such evidence. With the "Gesetz zur Reform der Zivilprozessordnung" (law for the reform of the code of civil procedure), which has become effective on 01.01.2002, there are special consequences in civil action regarding electronic signatures now. These aim particularly on the facilitation to make the proof of the receiver of a signed document easier [cf. Fischer-Dieskau/Gitter/Paul/Stedile 2002].

#### **4.1.3.1 Other Electronic Signatures and Advanced Electronic Signatures**

For the 'other electronic signature' as well as the advanced electronic signature there is the basic principle of free assessment of evidence by the judge with regard to these objects of appearance. There are no special proof regulations with respect to this. The proof can be easier in fact when using a digital signature. This confidence can be obtained by long experiences with the reliability of such methods or measurements of the suppliers [Roßnagel 2002].

#### **4.1.3.2 Qualified Electronic Signatures**

For the qualified electronic signature the new § 292a ZPO was edited. Therein it is called: "The appearance of genuineness of an explanation available in electronic form (§ 126a of the German civil law) resulting from an examination according to the signature law, can only be unsettled by facts that substantiate serious doubts that the explanation has been given willingly by the key owner."

This means that when there is a qualified electronic signature that was also tested positively, the court in principle assumes that this explanation has been made by the signature key owner. If the opposing party already denies a qualified electronic signature exists, the party which refers

---

to the validity has to prove the prerequisites. He has to prove the fulfilment of the prerequisites of a qualified signature according to § 2 no. 2 a) – d) and no. 3 a) and b) SigG. He is not obliged to do so, if the opposing party could not arouse doubt.

Initially the exclusive assignment of the signature to the signature key owner must be proven according to § 2 no. 2 a) SigG. Suppliers of qualified signatures have to rely upon their documentation in accordance with § 10 SigG.

The proof of identifiability of the signature key owner as in § 2 no. 2 b) SigG can fail because due to the restricted obligation to reproach for qualified signatures (§ 4 paragraph 1 SigV). The supplier is obliged to keep them for only five years after expiry of the validity of the certificate. There is no trustworthiness of the root authority as such either since qualified certification suppliers confirm their trustworthiness to themselves on their own and mutually.

Furthermore the probating party has to prove that the signature was created with resources, that one of the signature key owners can hold under his exclusive control. This can be difficult due to the shorter preservation period mentioned above.

The proof of purity (like § 2 no. 3 b) SigG) can then be problematic if the employed signature method in the meantime has been proven to be insecure. To prevent this, a regular re-evaluation of the signatures every six years can be recommended.

Evidence to prove the use of safe signature construction units as in § 2 no. 3b) SigG might arise from the documentation of the supplier. This also applies to the proof that the signature is based on a qualified certificate valid at the time of its production (§ 2 no. 3 a) SigG). The technical and administrative security of the supplier must hereby be explained by the probating party.

If the probating party succeeds proving these six points, the 'proof of appearance' that the explanation was given with the will of the key owner is valid in his favour. This is however only a 'proof of appearance'. The opposing party still can destroy this appearance by presenting facts which arouse a serious doubt that the signature key owner has given the intended statement.

For example the signatory could refer to the fact, that not he but someone else (e.g., a thief) has performed the signing process unauthorised. The obligations to take precautions have to be noticed by signatories according to § 6 no. 1 and 2 SigV.

Furthermore he could claim that not the actual data he signed has been shown to him. He also has to prove this.

#### **4.1.3.3 Qualified Electronic Signatures based on voluntary Accreditation**

Some broader proof relieves arise in the context of the use of accredited signatures if it is necessary to prove the appearance of the genuineness of a prepared explanation.

It is suspected according to § 15 paragraph 1 sentence 4 SigG, that suppliers of accredited signatures use only signature keys which can not be duplicated and the signature key can not be calculated from the signature or the signature examining key.

The identification of the signature key owner is possible for a longer time for users of accredited signatures because they are testable for 30 years after expiry (§ 4 paragraph 2 SigV). This also applies to the proof that the signature was created with soft- and hardware, which the signature key owners can hold under his exclusive control. Furthermore a trustworthy root authority exists with the RegTP and the publication of the public key of the supplier in the German "Bundesanzeiger".

The technical and administrative security of the supplier and the production of valid qualified certificates can end since this had already been proven certainty for the accreditation process.

## 4.2 Pseudonymity

### 4.2.1 Legal

In European law the desirability of the use of pseudonyms depends on the kind of communication. In the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) the use of pseudonyms is explicitly mentioned. It can be found in Consideration no. 9: "The Member States, providers and users concerned, together with the competent Community bodies, should co-operate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible".

This is brought up again in Art. 8 of the EU Directive on electronic signatures that provides an explicit right of the signatory to mention a pseudonym instead of his real name.

Also the EU Directive about the protection of privacy in the telecommunication sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997) initiates that "in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemised bills".

The Directive on privacy and electronic communications (Directive 2002/58/EC of 12 July 2002) makes an exception to the acceptance of anonymity and pseudonymity for purposes of direct marketing. You can read in Article 13 paragraph 4: "In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited." But this exception doesn't modify the basic principle of desirability of anonymity and pseudonymity by the European legislator.

### 4.2.2 Electronic / Digital Signature

The user can according to German law decide that instead of his name only a pseudonym is included into the certificate (cf. § 5 paragraph 3 SigG). No further personal data are taken then. Pseudonyms are indicated by the entry "PN" in the certificate. In a certificate user data are stored independent of the signature. They give information about the sender and his authorities to the receiver of the message signed electronically.

At least the 3rd outline for changes of the German public relations prescriptions is against signing with pseudonyms. In the outline (§ 3a VwVerfG) can be read: 'It is illegal to sign with a pseudonym which does not make possible the identification of the person of the signing key owner.'

Whether this covers qualified signatures with a pseudonym is not clear. An identification is at least possible for the supplier of the certificate about the person of the key owner.

---

## 4.3 Other Legal Material

### [Amendments to the US Constitution]:

Amendments to the US Constitution. The Ten Original Amendments: The Bill of Rights. Passed by Congress on September 25<sup>th</sup>, 1789. Ratified December 15, 1791:

- 1) Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.
- 2) A well-regulated militia, being necessary to the security of a free State, the right of the people to keep and bear arms, shall not be infringed.
- 3) No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.
- 4) The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
- 5) No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.
- 6) In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favour, and to have the Assistance of Counsel for his defence.
- 7) In suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.
- 8) Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.
- 9) The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.
- 10) The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

The first French constitution dates back to September 20<sup>th</sup> 1791 and established that: "The National Assembly, in the desire to found the French Constitution on the principles that the Assembly has recognised and stated, irrevocably abolishes those institutions that impaired liberty and equal rights. There is no longer nobility nor peerage, nor hereditary distinctions, nor distinctions of standing, nor feudal regimes, nor seigniorial justices, nor any of the titles, denominations and prerogatives deriving from the same, nor any order of chivalry, nor any or the corporations or decorations for which proof of nobility was required or that presupposed distinctions of birth, nor any other superiority, besides that of public officials in the performance of their functions. There is no longer sale or inheritance of any public office, There is no longer, for any part of the nation, or for any individual, any privilege or exception vis-à-vis the law common to all the French. There are no longer either guilds or corporations of professions, arts and trades. The law no longer recognises either religious vows or any other bond contrary to natural rights or to the Constitution.

## Fundamental conditions guaranteed by the Constitution

The Constitution guarantees, as natural and civil rights:

- 1) that all citizens are eligible for admission to positions and jobs, without any other distinction besides that of their qualities and capabilities;
- 2) that all charges will be equally divided among all citizens in proportion to their respective substance;
- 3) that like crimes will be punished with like punishments, without any distinction between individuals.

Similarly, the Constitution guarantees, as natural and civil rights:

- a) Each man's right to go, stay, and depart, without being able to be arrested or detained, if not in the ways determined by the Constitution;
- b) Each man's freedom to speak, write, print and publish his thoughts, without such writings being able to be subjected to any censorship or inspection prior to publication, and to exercise the religion to which he belongs;
- c) The citizens' right to gather together peaceably and unarmed, subjecting themselves to police laws;
- d) The freedom to submit individually signed petitions to the legally constituted authorities.

Article 9 – No officer of the public police force may enter a citizen's home, except for the purpose of executing police or court orders, or in the cases officially envisaged by law.

### [Spanish Constitution]:

Spanish Constitution (1992)

Article 17 [Personal Liberty]

- (1) Every person has the right to liberty and security. No one may be deprived of his liberty without observance of the provisions of this article and only in the cases and in the form prescribed by law.
- (2) Preventive arrest may not last more than the time strictly necessary for the investigations required to clarify events, and in any case, within a maximum period of 72 hours, the person detained must be freed or placed at the disposal of the judicial authority.
- (3) Every person arrested must be informed immediately, and in a way that is understandable to him, about his rights and the reasons for his arrest, and he may not be forced to make a statement. The assistance of an attorney for the arrested person is guaranteed during police and judicial proceedings under the terms established by law.
- (4) The law will regulate a process of habeas corpus so that any person who is illegally arrested may immediately be placed at the disposal of the judiciary. The maximum period of provisional imprisonment shall also be determined by law.

Article 18 [Honour, Privacy, Home, Secrecy of Communication]

- (1) The right of honour, personal, and family privacy and identity is guaranteed.
- (2) The home is inviolable. No entry or search may be made without legal authority except with the express consent of the owners or in the case of flagrante delicto.
- (3) Secrecy of communications, particularly regarding postal, telegraphic, and telephone communication, is guaranteed, except for infractions by judicial order.
- (4) The law shall limit the use of information, to guarantee personal and family honour, the privacy of citizens, and the full exercise of their rights.

Article 19 [Freedom of Movement]

Spaniards have the right to freely select their residence and to travel in the national territory. They also have the right to enter and leave Spain freely under the conditions established by law. That right cannot be restricted because of political or ideological motives.

---

## Article 20 [Specific Freedoms, Restrictions]

- (1) The following rights are recognised and protected:
  - a) To express and disseminate thoughts freely through words, writing, or any other means of reproduction.
  - b) Literary, artistic, scientific, and technical production, and creation.
  - c) Academic freedom.
  - d) To communicate or receive freely truthful information through any means of dissemination. The law shall regulate the right to the protection of the clause on conscience and professional secrecy in the exercise of these freedoms.
- (2) The exercise of these rights cannot be restricted through any type of prior censorship.
- (3) The law shall regulate the organisation and parliamentary control of the means of social communication owned by the State or any public entity and shall guarantee access to those means by significant social and political groups, respecting the pluralism of society and the various languages of Spain.
- (4) These liberties find their limitation in the respect for the rights recognised in this Title, in the precepts of the laws which develop it and, especially, in the right to honour, privacy, personal identity, and protection of youth and childhood.
- (5) The seizure of publications, recordings, or other means of information may only be determined by a judicial resolution.

## Article 21 [Assembly]

- (1) The right to peaceful, unarmed assembly is recognised. The exercise of this right does not require prior authorisation.
- (2) In the cases of meetings in places of public transit and of manifestations prior notification shall be given to the authorities, which can only forbid them when there are reasons based on disturbances of public order with danger for persons or property.

## Article 22 [Association]

- (1) The right to association is recognised.
- (2) Associations that pursue purposes or use methods that are classified as crimes are illegal.
- (3) Associations constituted under the provisions of this article must register for purposes of public information only.
- (4) Associations may only be dissolved or their activities suspended by virtue of a motivated judicial order.
- (5) Secret and paramilitary associations are prohibited.

## [Italy – Criminal Code]

### PERSONAL FALSEHOOD

#### Art. 494 – Deceptive impersonation (imposture)

Anyone who, in order to procure benefits for himself or others or to cause damage to others, misleads someone, by illegally impersonating another person, or by giving himself or others a false name, or false status, or a quality to which the law ascribes juridical effects, is punished, if the deed does not constitute another crime against public good faith, with imprisonment of up to one year.

#### Art. 495 – False statement or declaration to a public official on one's own identity or personal qualities or those of others.

Anyone who falsely declares or states to a public official, in a public deed, his identity or status or other qualities or the identity, status or other qualities of another person, is punished with imprisonment of up to three years. He who perpetrates this act in a statement due to be reproduced in a public deed is subject to the same punishment. The prison sentence is not less than one year:

- 1) If the statements concerned are in deeds concerning civil status.

2) If the false statement on one's identity, status and personal qualities is made by a defendant to the judicial authority, or if, by virtue of the false declaration, a criminal sentence is registered under a false name in police records. The punishment is reduced if the person making the false statement intended to obtain, for himself or for others, the issue of certificates or administrative authorisations under a false name, or containing other untruthful indications.

#### Art. 496 – False statements on the identity and personal qualities of one's self or of others

Anyone who, in cases other than those indicated in the previous articles, when questioned on his identity, status or other qualities or those of another person, makes untruthful declarations to a public official, or to a person appointed to perform a public service, in the exercise of the functions or service, is punished with up to one year of imprisonment or with a fine of up to one million Italian lire [€ 516.46].

#### Art. 497 – Fraud in obtaining issue of police-record certificates and illicit use of such certificates

Anyone who fraudulently procures a police-record certificate or another criminal certificate concerning another person, or uses it for a purpose other than that for which it is intended, is punished with imprisonment of up to six months or with a fine of up to one million Italian lire [€ 516.46].

#### Art. 498 – Usurpation [illicit use] of titles or honours

Anyone who abusively wears in public the uniform or distinctive marks of a public office or job, or of a political, administrative or judicial body, or of a profession for which a special official licence from the state is required, or abusively wears ecclesiastical clothing in public, is punished with a fine of from two-hundred thousand to two million Italian lire [€ 103.29-€ 1,032.90]. The same punishment is applicable to those who claim academic qualifications or titles, titles, decorations, or other public honours, or qualities inherent to any of the offices, jobs or professions indicated in the previous provision. An adverse ruling leads to publication of the sentence.

### **In California by PENAL CODE SECTION 530.5**

#### 530.5

- (a) Every person who wilfully obtains personal identifying information, as defined in subdivision (b), of another person without the authorisation of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information in the name of the other person without the consent of that person is guilty of a public offence, and upon conviction therefore, shall be punished either by imprisonment in a county jail not to exceed one year, a fine not to exceed one thousand dollars (\$ 1,000), or both that imprisonment and fine, or by imprisonment in the state prison, a fine not to exceed ten thousand dollars (\$ 10,000), or both that imprisonment and fine.
- (b) "Personal identifying information," as used in this Section, means the name, address, telephone number, driver's licence number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person.
- (c) In any case in which a person wilfully obtains personal identifying information of another person without the authorisation of that person, and uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

---

In the USA Federal Law: Identity Theft and Assumption Deterrence Act of 1998 18 U.S.C. § 1028 make it a federal crime when anyone knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

[Section IV – CRIMINAL OFFENCES AGAINST INVOLABILITY OF DOMICILE]

Art. 614 – Violation of domicile

Anyone who enters another's home, or another place of private residence, or the appurtenances of the same, against the express or tacit desire of the subject having the right to exclude him, or who enters covertly or by means of subterfuge, is punished with imprisonment of up to three years. The same punishment is applicable to the person who remains in the aforesaid places against the express wish of the subject having the right to exclude him, or remains therein covertly or by means of subterfuge. The crime is punishable upon filing of a suit by the victim. The punishment ranges from one to five years [of imprisonment] and proceedings are automatically initiated by the authorities if the deed is committed with violence against objects or persons, or if the guilty party is manifestly armed.

Art. 615 – Violation of domicile by a public official

Any public official who, abusing of the powers inherent to his functions, enters or remains in the places indicated in the previous article, is punished with imprisonment of from one to five years. If the offence consists of entry of the said places without observing legally established formalities, the punishment is imprisonment for up to one year.

Art. 615/2 – Illicit interference in private life

Anyone who, via the use of visual or audio recording equipment, unlawfully procures news or images pertaining to private life occurring in the places indicated in Article 614, is punished with imprisonment of from six months to four years. Also subject to the same punishment, unless the deed constitutes a more serious offence, are those, are those who reveal or divulge to the public, via any news medium, the news or images obtained in the ways indicated in the first part of this article. The offences are punishable upon filing of suits by victims. However, proceedings are automatically initiated by the authorities, and punishment is imprisonment of from one to five years, if the deed is committed by a public official or by a person appointed to perform a public service, with abuse of powers or infringement of the duties inherent in the function or services, or by a person who exercises, also illicitly, the profession of private detective.

Art. 615/3 – (Improper access to a computer or remote electronic communications system)

Anyone who improperly enters a computer or remote electronic communications system protected by security measures or who remains therein against the express or tacit wish of the subject having the right to exclude him is punished with imprisonment of up to three years.

The punishment is imprisonment of from one to five years:

- If the deed is committed by a public official or by a person appointed to perform a public service, with abuse of the powers or infringement of duties inherent to the function or service, or by a person exercising, also illegally, the profession of private detective, or abuses of the quality of system operator
- If, in order to commit the offence, the guilty party commits violence against objects or persons, or is manifestly armed

- If the deed causes destruction of or damage to the system or total or partial interruption of its operation, or destruction of or damage to data, information, or programs contained (in the system)

If the deeds indicated in the first and second paragraphs concern computer or remote electronic communications system of military interest, or concern public order, public safety, or health, or public civil protection, or in any case the public interest, the punishment is, respectively, imprisonment from one to five years and from three to eight years.

In the case envisaged in the first paragraph the offence is punishable upon filing of a suit by the victim. In the other cases, it is subject to proceedings automatically initiated by the authorities.

[APPENDIX: "Constitutions references to privacy protection"]

**Article 28 Constitution of Ukraine:**

Everyone has the right to respect of his or her dignity.

No one shall be subjected to torture, cruel, inhuman or degrading treatment or punishment that violates his or her dignity. No person shall be subjected to medical, scientific or other experiments without his or her free consent.

**Article 47 Constitution of Poland:**

Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life.

**Article 32 of Bulgaria:**

- (1) The privacy of citizens is inviolable. Everyone is entitled to protection against any illegal interference in his private or family affairs and against encroachments on his honour, dignity, and reputation.
- (2) No one shall be followed, photographed, filmed, recorded, or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law.

**Article 35 Constitution of Slovenia:**

The physical and mental integrity of each person shall be guaranteed, as shall be his right to privacy and his other personal rights.

**Article 59 Constitution of Hungary:**

- (1) In the Republic of Hungary everyone has the right to the good standing of his reputation, the privacy of his home and the protection of secrecy in private affairs and personal data.
- (2) A majority of two-thirds of the votes of the Members of Parliament present is required to pass the law on the secrecy of personal data.

**In the extra-Europe Constitutions:**

**Article 14 Constitution of South Africa:**

Everyone has the right to privacy, which includes the right not to have -

- (a) their person or home searched;
- (b) their property searched;
- (c) their possessions seized; or
- (d) the privacy of their communications infringed."

**Article 30 Constitution of Hong Kong:**

The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in

---

accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.

**Article 33 Constitution of Paraguay:**

- (1) Personal and family privacy, as well as the respect of private life, are inviolable. Individual behaviour that does not affect public order as established by law or the rights of third parties is exempted from the authority of public officials.
- (2) The protection of the privacy, dignity, and private image of each individual is hereby guaranteed.

**[Crime against honour]**

**Article 137 c. to g. Dutch Penal Code:**

Art. 137 c.: A person who publicly, either orally, or in writing, or by image, intentionally makes a defamatory statement about a group of persons on the grounds of their race, religion or personal beliefs, or their hetero- or homosexual orientation, is liable to a term of imprisonment of a period of not more than one year or a fine of the third category.

Art. 137 d.: A person who publicly, either orally or in writing or by image, incites hatred of or discrimination against persons or violence against their person or property, on the grounds of their race, religion or personal beliefs, their sex or their hetero- or homosexual orientation is liable to a term of imprisonment of not more than one year, or a fine of the third category.

Art. 137 e.:

1. A person who, for any reason other than giving factual information:

Makes public a statement which he knows or should reasonably suspect to be offensive to a group of persons on the grounds of their race, religion, or personal beliefs, or their hetero- or homosexual orientation, or incites hatred of or discrimination against people or violence against their person or property on the grounds of race, religion or personal beliefs, their sex or their hetero- or homosexual orientation:

Disseminates an object which he knows or should reasonably suspect to contain such defamatory statement or has such in stock for public disclosure or for dissemination; is liable to a term of imprisonment of not more than six months or a fine of the third category.

2. Where the offender commits any of the offences defined in this article in the practice of his profession, and where, at the time when the serious offence is committed, less than five years have passed since the previous conviction, of the offender for any of these offences became final, he may be disqualified from the practice of that profession.

Art. 137 f.: A person who takes part in activities, or who extends financial or other material support to activities, aimed at discrimination against persons on the grounds of race, religion or personal beliefs, their sex or their hetero- or homosexual orientation: orientation is liable to a term of imprisonment of not more than three months, or a fine of the second category.

Art. 137 g.: A person who in his official capacity, profession or business, intentionally discriminates against persons on the grounds of their race, religion, or personal beliefs, or their hetero- or homosexual orientation, or incites hatred of or discrimination against people or violence against their person or property on the grounds of race, is liable to a term of imprisonment of no more than six months or a fine of the third category.

**California Civil Code**

§ 45 – Libel: Libel is a false and unprivileged publication by writing, printing, picture, effigy, or other fixed representation to the eye, which exposes any person to hatred, contempt, ridicule, or obloquy, or which causes him to be shunned or avoided, or which has a tendency to injure him in his occupation.

§ 46 – Slander: California Civil Code § 46 – Slander: Slander is a false and unprivileged publication, orally uttered, and also communications by radio or any mechanical or other means which:

1. Charges any person with crime, or with having been indicted, convicted, or punished for crime;
2. Imputes in him the present existence of an infectious, contagious, or loathsome disease;
3. Tends directly to injure him in respect to his office, profession, trade or business, either by imputing to him general disqualification in those respects which the office or other occupation peculiarly requires, or by imputing something with reference to his office, profession, trade, or business that has a natural tendency to lessen its profits;
4. Imputes to him impotence or a want of chastity; or
5. Which, by natural consequence, causes actual damage.