1 Introduction

Kai Rannenberg, Denis Royer, and André Deuker

The value of identity of course is that so often with it comes purpose.
Richard Grant

The ever increasing digitisation of information has led to an Information Society, in which more and more information is available almost anywhere and anytime. The related digitisation of personal characteristics and personal information is progressively changing our ways of identifying persons and managing our relations with them especially in virtual interactions, e.g., over the Internet. As the Internet has opened new spaces for (virtual and supplementary) lives, supplementary digital identities, so-called virtual identities are being created for reasons of security, profit, convenience or even fun (e.g., for leisure communities). What used to be a 'natural' identity, e.g., the personal appearance of an individual at a counter, is now as virtual as a user account at a web portal, an email address, or a mobile phone number. These virtual and multiple identities and the paradigms behind them are feeding back into the 'physical' world, offering a mix of physical and virtual plural identities and processes to deal with them. Both the new artefacts as well as the new processes challenge the traditional definitions of identity.

At the same time identities are subject to diverse forms of management in business, administration, and among citizens: There is almost no week, which does not see a new initiative aiming at 'better' identification of citizens, customers, consumers, or entities in general. In this context 'better' can have many different meanings, often depending from the point of view of the respective stakeholder: States and their administrations try to identify 'their' citizens, while citizens want to be able to influence the respective identification, e.g., its rationale, its degree, its process and last but not least the information flow around it, starting with the question whether or not identification is needed for a transaction or for participating in a certain element of life in society. The core question and often the source of conflict is who owns how much identity information of whom and who needs to place trust into which identity information to allow access to resources.

While this book cannot answer all questions related to identity it presents some relevant results from the EU funded research project FIDIS (Future of Identity in the Information Society). This chapter is an introduction to the book. It first raises some exemplary issues of identity and its application in a changing world, describing the role and aim of FIDIS in this situation. Following this, a

short overview of the respective parts of the book (also as a look in to the engine room of FIDIS) is presented, before the chapter is concluded with the thanks and acknowledgements.

1.1 Identity in a Changing World

For a long time identity has been an issue of thought and analysis, as well as of doubt and crisis. Now also in the Information Society, identity is becoming an issue of discussion and sometimes major conflict. One of the basic questions is, whether entities have one single identity or several (*partial*) identities. As an introduction into the topic this section discusses the question of '*One identity or many*' first in general terms and then in typical examples of the information society.

1.1.1 One Identity or Many? Identity Unification vs. Identity Differentiation

Having one single (continuous) identity has for long been viewed as a sign of integrity of character and of health of personality: In contrast an identity crisis is diagnosed, when an individual loses a sense of personal sameness and historical continuity. Also in the information society, whoever feels the need to better identify and address related entities is on the verge of identity unification by identity management.

Nowadays, employees in an organisation very often have a historically grown plethora of identifiers and access rights. Consequently it is difficult to know and manage, who has the authorisation to do what. So when someone leaves an organisation it is usually difficult to revoke authorisations, accounts and access rights to avoid later misuse of corporate systems and corporate information. Establishing an efficient framework for corporate access management with reliable accountability is not a trivial task. A popular aim here is 'single sign-on', basically the unification of all accounts and access rights on one system per enterprise, to which users authenticate themselves and which then provides access to the resources needed, such as a customer database or a printer.

A similar unification approach is popular in dealing with customers, e.g., when a telecommunication company unifies customers' accounts to provide a single bill for different but related services. Currently very often a provider offers landline telephony, mobile telephony, and Internet access – and sends a different bill for each. Whereas this may cause unnecessary costs and complexity, the unification of those accounts that refer to the same customer also offer the chance to provide more customised and personalised bundled services while raising the security, service quality, and customer satisfaction.

The unification of accounts and access rights can be a double-edged sword for users and service providers alike. Users usually like the added convenience of single-sign-on systems, using one single password for a number of log-ins and

access accounts. Enterprises on the other hand see the benefit of single sign-on systems in a better control and management of access rights. However, as the number of applications for one individual increases, adding numerous mobile devices or new web-based services to their daily life, the risk of data misuse increases as well. The idea of just having to provide a fingerprint instead of typing a complicated password every morning is fascinating. However, the more sensitive information gets possibly accessed with this one identifier, the higher the risk for the user to fall victim to identity fraud and ultimately experience loss or damage.

A similar scenario applies to the service provider. When it comes to personal information stored on computer systems, privacy concerns need to be taken seriously. It may well be useful for a citizen to have an account with the tax office to deal with the annual tax declaration online, and it may be useful to link this with some information on the costs paid for medical services, but e.g., a complete unification of all the data and profiles stored by the tax office, the hospital, and the health insurance would need to be managed closely and is unacceptable in many cultures – besides the fact that it may violate privacy regulations. Very often Internet accounts, such as eBay or YouTube accounts, are named in a way that does not give a hint towards their holders 'normal' names or email addresses. These accounts serve as partial identities supporting users, who want more control over their identity and over personal information which is collected and stored on them. They also want to be able to use technologies for anonymity and pseudonymity in order to manage whether and how they are identified in which contexts. Consequently 'Identity Differentiation' is another major trend in more or less direct contrast to 'Identity Unification'.

1.1.2 Identity in Different Areas of the Information Society

The looming conflicts can be seen in the changing world of 'classic' physical and organisational entities, such as citizens, governments, customers, businesses employees, and enterprises, and the relation(s) between them. This is due to new and ongoing political developments, such as the integration of the European Union, and due to new and ongoing economic trends, such as global competition, global sourcing, and the disintegration of traditional value chains. All these trends have a strong influence on the respective identities, as can be seen in the discussion of the following areas.

Citizens and Their Governments ('G2C')

European states still follow very different concepts of identification and identity management: E.g. in Germany holding an ID card is mandatory for any citizen from 16 years of age on, while in the UK any initiative towards state-issued identity cards creates major discussion and even uproar in society. On the other side social acceptance of CCTV, a rich base for investigating where people are at

which point in time or who has been at a location at a certain time is much more popular in the UK than in Germany.

While Europe is only in the process of merging its identity cultures and processes the raising connectivity and the Internet bring a new dimension into the discussion: A hotel, that would not only take the ID-Card or passport of an arriving guest, but would also routinely double-check these documents with the issuing authorities would create at least raised eyebrows if not astonishment. In the Internet this is a common practice: Somebody being asked for granting access sees itself as a relying party and checks identifiers (e.g. certificates, credit card numbers, or other credentials) immediately and directly with the parties who issued these identifiers.

Meanwhile there are discussions among providers of physical ID-Cards to establish a service for on-the-spot-double checking of physical ID-Cards presented to relying parties, such as hotels. This could help to identify criminals and other parties being searched for. Public-private partnerships for offering these services more efficiently are being discussed. The unification of identifiers would help these initiatives a lot.

However, the way how identities and identifiers are handled has a close relation to the way how citizens are treated and therefore to the essence of our democracies. The question is, whether citizens are per se considered to be criminals that need to be identified as thoroughly as possible, or whether they are considered to be able to select adequate partial identities, identifiers and the degree of identification in a situation.

Business and Their Customers ('B2C')

Many milestones of social development came along with major changes in the economy. The rise of the Information Society is closely related to the evolution of the ICT industry and the diffusion of ICT in everybody's life. Yet, the Information Society tends towards something that can be characterised as an information affluent society, where more information than needed is available. For businesses it is not just the goal of reaching the (potential) customer – gaining the customers' attention is the real deal. As a result, products, services, and communication are increasingly tailored towards the demands and requirements of individual customers or groups of them.

While customers' attention is becoming the scarce resource, identification of customers and knowledge about their identity attributes is getting more and more of a major asset for businesses. Depending on business area and business model, the role of identity can be manifold within the process of value creation. Traditionally, identification and identity plays a major role within the payment process, e.g., for judging of customers' creditworthiness. Knowledge about customers' identity has always been a central part of customer relationship programs. Nowadays and in addition to the classical applications, identity attributes are more and more used to better sell or create products in the online world:

- Online retailers use customer preferences to recommend goods and services.
- Individualised advertising within social networks and communities is based on identity attributes stored within user profiles.
- Automatic pricing of goods and services depending on customers' identity attributes is possible and has already been tested.

Knowledge about customers' identities will play a prominent, if not even central role in future processes of value creation. Handling identities in a proper way to prevent the invasion of customers' private spheres will be one major challenge for businesses to keep the relationship with their customers alive.

Enterprises and Their Employees ('B2E')

Today's digital work environments include more and more (business) processes facilitated by information systems. Organisations have to take care of their users and access management (often called identity and access management (IAM)), in order to protect their systems and their information from unauthorised access and to lower their overall costs (e.g., by centralising account data of various information systems). The need for these initiatives is enforced by the diversity of IT infrastructures used in everyday transactions (e.g. enterprise resource planning, document management, or human resources management) and the often dynamic change in user entitlements, (e.g., due to job changes, promotions, or layoffs). Therefore, identity management systems (IdMS) are becoming increasingly important for companies and corporations, and given enterprise-wide responsibilities these need to be enterprise-wide identity management systems.

A variety of identity management technologies can be identified. Examples are single / reduced sign-on, directory services, public-key infrastructures, and IAM systems. Still and contrary to the position of many technology vendors identity management is not a simple out-of-the-box solution but a complex framework of different technologies and functions. So when introducing IdMS, organisations incur a variety of costs for the implementation and the related organisational issues, such as the integration of processes and technologies.

Therefore, topics such as the interoperability of IdMS, business process integration of identity related technologies, and High-Tech ID (RFID tokens, biometry, etc.) are in the focus of interest. While the technology issues seem to be a solvable problem, practical challenges and research needs to follow from the complex interaction of the various players, processes, structures, and tasks of organisations.

1.2 The Role of FIDIS

FIDIS (Future of Identity in the Information Society, www.fidis.net) is a multidisciplinary endeavour of 24 leading institutions from research, government, and industry. Research from states with different cultures on e.g., the identification of

citizens and ID cards is combined towards a well-founded analysis of High-Tech IDs and Virtual Identities, considering aspects, such as privacy, mobility, interoperability, profiling, forensics, and identity related crime. It is organised as a Network of Excellence (NoE) in the 6th Framework programme of the European Union, funded under Contract N° 507512.

The borders between the scenarios and the concepts of identity as well as identity management, etc. are not sharp lines and cannot be sharp lines. Overlaps exist almost everywhere, making identity omnipresent.

Identification and authentication, identity management, liability, security and privacy, legal aspects, and social implications are issues that need to be carefully addressed by researchers and policy makers. The main aspects of these are being analysed in depth by the FIDIS 'Future of Identity in the Information Society' Network of Excellence (NoE), which is also working on the issues' complex interactions, a difficult and important task requiring the integration of inter-disciplinary expertise.

FIDIS is proud to contribute to the future of identity in the Information Society, e.g., by shaping the requirements, definition, conception and development of specific security, trust and privacy technologies, and infrastructures. This should help to enable a joint or at least synchronised European approach for identity management.

1.3 On This Book

When FIDIS came into existence there was confidence that it would produce results that deserve reading beyond the usual lifetime of a project deliverable, even though one at that time did not exactly know what they were. So the idea to summarise the results after 5 years was always around. Now the book in your hand aims to give an overview of those results that FIDIS considered to be most interesting.

For many chapters this means that the respective work package leaders edited them, while other were joint editing efforts by FIDIS partners and / or FIDIS coordination. This introduction aims to give some guidance through the flow of topics and chapters in this book that aims to document the most relevant aspects of identity and its future challenges and opportunities.

The remainder of this section is structured as follows: Three subsections give an overview on the main scientific chapters of the book. A forth subsection introduces the 'Vignettes', short hypothetical scenarios to illustrate future impacts of identity developments on the daily lives of ordinary people, and a fifth subsection explains the Annexes of the book.

1.3.1 Basic Concepts

Chapter 2 introduces foundational concepts on the 'Identity of Identity'. The objective of this chapter is not to bring the ultimate answer to the question 'What is identity?', as this would be an almost impossible undertaking given the complex-

ity and the constant evolution of the subject. The aim is rather to present different angles that can be used to define the concept, in particular in the context of the Information Society. Starting at describing how this conceptualisation can be conducted in the traditional way of theorisation well known by academics, this chapter then indicates how less formal approaches such as narratives can be used to help understand the concept. It also introduces how the new 'social tools' originating from the 'Web 2.0' can be used to stir the intelligence of experts from different horizons so as to generate a meaningful and practical understanding of the subject. The second part of Chapter 2 illustrates how each of these approaches has been operationalised by presenting a series of models and scenarios presenting different perspectives and issues that are relevant to the subject, and a collaborative Web 2.0 knowledge infrastructure that is used in FIDIS to facilitate the conceptualisation of identity by a group of experts.

Chapter 3 introduces the concept of 'Virtual Persons and Identities', bringing light to the questions: 'What is a virtual person? What is it used for? What is its added value?'. Virtual persons sometimes describe avatars and new forms of identities in online games. They also appear in other contexts (e.g., in the legal domain). Within the work of FIDIS, the concept of virtual persons has been extended to better describe and understand new forms of identities in the Information Society in relation to rights, duties, obligations and responsibilities.

Virtual persons, as other virtual entities, exist in the virtual world, the collection of all (abstract) entities, which are or have been the product of the mind or imagination. The virtual world – not to be confused with the digital world – allows a unified description of many identity-related concepts that are usually defined separately without taking into consideration their similarities: avatars, pseudonyms, categories, profiles, legal persons, etc.

The legal system has a long experience of using abstract entities to define rules, categories, and the like in order to associate legal rights, obligations, and responsibilities to persons that can be considered instances of these abstract entities in specific situations. The model developed within FIDIS and lined out in this chapter uses a similar construction. After introducing the model, the application to pseudonyms is described. Also the concept of virtual persons from a legal perspective and (eventually) trust in the light of virtual persons is explored.

1.3.2 Identity and Advanced Technologies

Turning towards technologies to facilitate the management of identities, Chapter 4 analyses High-Tech ID and emerging technologies. Technological development has undeniably pervaded every aspect of our lives, and the ways in which we now use our identity related information has not escaped the impact of this change. We are increasingly called upon to adopt new technology, usually more through obligation than choice, to function in everyday society, and with this new era of supposed convenience has come new risks and challenges. Chapter 4 examines the technological roots of identity management and the systems used to support this

activity, means to protect digital information (such as public-key encryption) and digital signatures and the evolving yet somewhat controversial role of biometrics in identification and authentication.

Considering the ever changing landscape of identity related technologies, Chapter 4 further explores emerging technologies with likely impact in the near to mid-term future. These include Radio Frequency Identification (RFID) which has more recently come to the fore of the public consciousness, Ambient Intelligence environments which offer convenience at the potential cost of privacy and human implants which surprisingly have already been developed in a medical context and look set to be the next major step in our ever burgeoning relationship with technology.

Chapter 5 turns to another sometimes underestimated technology related to identity management: While identity management systems for the Internet have been debated intensively, identity management in mobile applications has grown silently over the last almost 20 years. Technologies, such as the still-growing Global System for Mobile Communication (GSM) with its Subscriber Identity Module (SIM) identification infrastructure, are foundations for many new mobile identity management related applications and services. This includes location-based services (LBS), offering customised and convenient services to users (e.g., friend finder applications) and new revenue opportunities for service providers (e.g., location-based advertising).

However, even though the opportunities seem to be endless and technology manageable, challenges arise when looking at advanced aspects of mobility and identity such as privacy, regulation, the socio-cultural aspects, and the economic impacts. To this regard, the interdisciplinary nature of mobility and identity is imminent and needs to be explored further. By learning from the diverse field of challenges, new mobile communication systems can be created, allowing for more privacy-preserving service provision and a more transparent handling of mobile identities. Therefore Chapter 5 presents an analysis of the specific properties of Mobile Identities, leading to a description of the FIDIS perspective on mobility and identity. Then a deeper analysis of the technological aspects of mobile networks gives the basis for a closer look from the legal perspective (on issues such as data protection), the sociological, and the economic perspective. An outlook on the future challenges of mobility and identity concludes this chapter.

One of the key aspects of effective and efficient management of identities is interoperability, being the focus of Chapter 6. Establishing interoperable systems is a complex operation that goes far beyond the technical interconnectedness of databases and systems. Interoperability emerges from the need to communicate data across different domains for a specific purpose. Transferring the data may represent a technical challenge because of different protocols, standards, formats and so forth. However, the most difficult challenge lies in reconciling and aligning the purpose, use and other changes consequent on transferring that data. Changes in data ownership and custodianship have an effect on power structures, roles and responsibilities and on risk. In the first part of this chapter our aim is to develop an understanding of the term interoperability as it currently applies to the area of

identity management. FIDIS proposes a three-fold conception of interoperability in IdMS, involving technical, but also formal-policy, legal and regulatory components, as well as informal-behavioural and cultural aspects. Having noted the official EU / government agenda as regards interoperable IdMS, the second part of the chapter is concerned with the perspective of other important stakeholders on the same topic. First, the views of experts from private and public sectors across Europe are presented. Following this, the perceptions and attitudes of EU citizens towards interoperable IdMS are discussed. Together, the findings presented point to the crucial challenges and implications associated with the sharing of personal data in the provision of eGovernment, eHealth, and related services.

1.3.3 Identity and Society

Some of the most critical challenges for 'the future of identity in information society' must be located in the domain of automated profiling practices, being the focal point of Chapter 7. Profiling technologies enable the construction and application of group profiles used for targeted advertising, anti-money laundering, actuarial justice, etc. Profiling is also the conditio sine qua non for the realisation of the vision of Ambient Intelligence. Though automated profiling seems to provide the only viable answer for the increasing information overload and though it seems to be a promising tool for the selection of relevant and useful information, its invisible nature and pervasive character may affect core principles of democracy and the rule of law, especially privacy and non-discrimination. In response to these challenges Chapter 7 suggests novel types of protection next to the existing data protection regimes. Instead of focusing on the protection of personal data, these novel tools focus on the protection against invisible or unjustified profiling. Finally, Chapter 7 develops the idea of Ambient Law, advocating a framework of technologically embedded legal rules that guarantee a transparency of profiles that should allow European citizens to decide which of their data they want to hide, when and in which context.

With the ever-increasing use of identities in commercial transactions, such as credit card payments, identity-related crime is also on the rise. Combating crimes like identity fraud, not in the least with the help of identity forensics, is a key challenge for policy makers. Therefore Chapter 8 aims at contributing to addressing that challenge. It summarises the findings of five years of FIDIS research on identity-related crime and identity forensics. A typology is given of the various forms of identity-related crime. After an analysis of relevant socio-economic, cultural, technical, and legal aspects of identity-related crime, potential countermeasures are discussed. We then move on to forensic aspects, with a critical analysis of pitfalls in forensic identification and case studies of mobile networks and biometric devices. Next, forensic profiling is discussed from a wide range of perspectives. The chapter concludes with lessons drawn in the area of identity-related crime and forensic aspects of identity.

Last but not least, the relation between privacy and identity is the main topic of Chapter 9. The current mainstream approach to privacy protection is to release as

little personal data as possible ('data minimisation'). To this end, Privacy Enhancing Technologies (PETs) provide anonymity on the application and network layers, support pseudonyms and help users to control access to their personal data, e.g., through identity management systems. However, protecting privacy by merely minimising disclosed data is not sufficient as more and more electronic applications (such as in the eHealth or the eGovernment sectors) require personal data. For today's information systems, the processing of released data has to be controlled ('usage control'). This chapter presents technical and organisational solutions elaborated within FIDIS on how privacy can be preserved in spite of the disclosure of personal data.

As initially stated, even after 5 years of FIDIS, not all questions in the domain of identity and identity management could be answered completely This is due to the fact that identity is a moving target, which is constantly evolving in different directions. Consequently, the concluding Chapter 10 presents the open challenges and potential (especially for Europe) on how to deal with the issues of identity.

1.3.4 The Vignettes

As an addition to the more scientifically oriented Chapters described so far FIDIS has developed a number of hypothetical scenarios which illustrate potential future identity developments as well as their potential impact on the daily lives of ordinary people. These scenarios are placed as 'Vignettes' between the 'scientific' chapters.

Based on the results of FIDIS Deliverable on use cases and scenarios of emerging technologies[1], the scenarios are heavily influenced and triggered by the endeavours of FIDIS and the personal experiences and expectations of the authors. Of course, the future is always clouded in uncertainty and the goal of each scenario is not to deliver the most accurate prediction of the future at all. Nonetheless, visions and hypotheses of individuals have always been a first step towards a next stage of technical, economical or social development – most likely also for the future of identity in the information society.

Starting with a scenario that looks at the potential impact of Ambient Intelligence environments, a subject well explored in the FIDIS network, subsequent scenarios focus on biometrics, social networks, virtual identities, grid computing and forensics, all areas to which FIDIS has dedicated much research effort.

A number of characters show up in the scenarios, among them Frank Idis, a 39-year-old humanities teacher and housemaster at a British public school in Royston Vasey, in the north of England. He first met his now wife Fanny (née Cheung) while holidaying in mainland Greece. Fanny's family are originally from Hong Kong, but she is second generation in the UK. Fanny works as a security director of a big hotel chain and frequently visits companies producing security devices.

[1] Gasson, M. (ed.) (2008), FIDIS Deliverable D12.5: Use cases and scenarios of emerging technologies.

1.3.5 The Annexes

This book aims not only at comprising the core results of FIDIS, but also to give an insight into FIDIS' way of work. Therefore the deliverables (Annex A) as well as the biographies of the contributors (Annex B) and the descriptions of the partners (Annex C) are included. Last but not least and as an example of outreach activities beyond the core activities of FIDIS Annex D contains a joint paper with two major thought-leaders in the identity arena (Kim Cameron (Microsoft) and Reinhard Posch (TU Graz, Government of Austria) on a 'Proposal for a common identity framework: A User-Centric Identity Metasystem'.