

The Future of Identity in the Information Society

Kai Rannenberg • Denis Royer
André Deuker
Editors

The Future of Identity in the Information Society

Challenges and Opportunities

Editors

Prof. Dr. Kai Rannenberg
Denis Royer
André Deuker

Goethe University Frankfurt
Institute of Business Informatics
Chair for Mobile Business and Multilateral Security
Grüneburgplatz 1
60629 Frankfurt am Main
Germany
Kai.Rannenberg@m-chair.net
Denis.Royer@m-chair.net
Andre.Deuker@m-chair.net

ISBN 978-3-540-88480-4
Springer Dordrecht Heidelberg London New York

Library of Congress Control Number: "PCN applied for"

© Springer-Verlag Berlin Heidelberg 2009

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permissions for use must always be obtained from Springer. Violations are liable for prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Cover design: WMXDesign GmbH

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

During the past decade the Information Society has firmly established itself in Europe and elsewhere, and ICT has deeply and irreversibly dyed the economic and social fabric of society. A stage of development has been reached that is characterised by massive amounts of personal data being generated, collected, analysed and processed, exchanged, recombined, and stored sometimes for a life-time or more. The contours of the digital age have rapidly taken shape and with this, the creation and management of individual identity has emerged as one of the central challenges in digital life. Citizens look for value in the activities they do on the Internet. Therefore they want to be able to trust the technology and services provided and the actors behind it. For that trusted electronic identity management is crucial.

On-line services can provide a lot of benefits and convenience to citizens and huge competitive advantages to European industry. Yet for such services to enjoy large-scale growth, people and organisations must have sufficient confidence that their personal dignity and legitimate business interests are properly safeguarded. It goes without saying that Europe needs an innovative and competitive ICT services sector to meet the challenges of the digital economy, to remain competitive and to foster investment, growth and jobs. This can only be successful if it is based on a privacy protecting ID management framework providing authentication mechanisms that protect human dignity, ensure protection against malicious behaviour and deceit, and allow for accountability and liability, and hence the rule of law in digital space. Europe's strong social values must be transferred to future digital life.

Trust in the use of eServices, in digital communications and applications, in eCommerce, eHealth, eGovernment, and ensuring the free movement of knowledge – the so-called “Fifth Freedom” – and open collaboration is evolving with society. There is no single ‘silver bullet’ solution to information identity risks. To achieve a true European culture of trust and security in digital life, decision-makers in business and government, regulators and technology developers must work together in a multi-stakeholder dialogue to find the right mix of methods, technology and regulation. In this respect, I would like to point to the Commission's policy initiative “i2010 – A European Information Society for growth and employment”. i2010 identifies security, in a broad sense including trust and privacy, as one of the four main challenges posed by digital convergence, which is at the heart of the creation of the single European Information Space. Furthermore trust, identity management and privacy protection are strong elements in European supported research, organised within the broader Framework Programme for Research and Development of the European Union.

Our society calls for diversity, openness, interoperability, usability and competition as key drivers for trust and security. Diversity reduces the risk stemming from the dependence on one type of technology and introduces natural safeguards. Open standards and interoperability are key to competition and for empowering users to freely choose products and services that they find useful, and for creating business opportunities for small, medium and large companies alike.

FIDIS has put Europe on the global map as a place for high quality identity management research. It has, together with several other EU supported activities, effectively contributed to creating the conditions for a flourishing digital economy and digital life, which are key aims of the Commission's regulatory and research policy.

I would like to thank the FIDIS project and all contributors to this "FIDIS Summit Book" for the opportunity to draw attention to the European Commission's efforts in this domain, and for putting Europe on the map as a global thought leader in privacy protective digital identity management. The fact that the Summit Event takes place in Cyprus – one of the recent EU Member States – is to be seen as a tribute to the shared European values of democracy, freedom and civil liberties.

Brussels, March 2009

Viviane Reding
Member of the European Commission,
Responsible for Information Society and Media

Acknowledgements

Editing and writing a multidisciplinary book like the one at hand is not something that is possible without ‘an army’ of helping hands that dedicated their knowledge, expertise, and time to make the work a success. Among the countless people that worked on this FIDIS volume, we would like to give a special thanks to:

- The partners, chapter editors, and researchers in the NoE FIDIS that contributed to this book and the deliverables (cf. Annex A) this book is based on.
- The reviewers of the chapter that dedicated their time to improve and streamline the different chapters.
- The people that helped to create this book:
 - Birgit Leick and later Christian Rauscher at Springer for helping us publish this piece of work.
 - George Scott for transforming much of the Englishish in the draft versions of this book into English.
 - Markus Richter for making this book agreeable to the eye.
 - Frieder Vogelmann for all sorts of trouble-shooting.
 - Our colleagues at the Chair of Mobile Business and Multilateral Security at Goethe University Frankfurt for keeping our backs covered when producing this book.
- The European Commission for funding FIDIS, as well as its Project Officers (Dirk van Rooy, Günter Schumacher, Richard Sonnenschein, Alain Jaume) and their management (Jacques Bus, Gerald Santucci, Andrea Servida), who kept up with whatever developments and challenges such a large and lively network is putting up.
- Last but not least Stefan Figge, without whom the successful FIDIS proposal would have never come into existence.

Frankfurt am Main, February 2009

Kai Rannenberg
Denis Royer
André Deuker

Table of Contents

1	Introduction	1
	<i>Kai Rannenberg, Denis Royer, and André Deuker</i>	
1.1	Identity in a Changing World	2
1.1.1	One Identity or Many? Identity Unification vs. Identity Differentiation	2
1.1.2	Identity in Different Areas of the Information Society	3
1.2	The Role of FIDIS	5
1.3	On This Book	6
1.3.1	Basic Concepts	6
1.3.2	Identity and Advanced Technologies	7
1.3.3	Identity and Society	9
1.3.4	The Vignettes	10
1.3.5	The Annexes	11
	VIGNETTE 1: PUTTING THE MACHINES IN CONTROL	13
2	Identity of Identity	19
	<i>Thierry Nabeth</i>	
2.1	Defining the Identity Concept	19
2.1.1	The Multidisciplinary Challenge	20
2.1.2	Identity: A Concept Subject to Major Evolutions	21
2.1.3	Addressing the Challenges	23
2.1.4	Structure of This Chapter	24
2.2	Conceptualisation	24
2.2.1	Formal <i>versus</i> Informal Conceptualisation	25
2.2.2	Formal (or Explicit) Conceptualisation	26
2.2.3	Informal Conceptualisation with Narratives	29
2.2.4	Web 2.0 & Conceptualisation with Wikis, Blogs, Social Bookmarking and Other Tools	31
2.3	Identity of Identity Defined (Formal Conceptualisation)	35
2.3.1	The Concepts of Identity and Identification	36
2.3.2	(Self-)Identity Concepts. Some Models	39
2.3.3	Terminology of Identity	42
2.3.4	Profiles of the Person, and Overview	44

2.4	Identity Use Cases and Scenarios	48
2.4.1	Virtual Online Social Environments, Real Identities Issues	49
2.4.2	Real Life in Virtual Worlds – Anthropological Analysis of MMO Games	52
2.4.3	Enjoy a Bar in 2012	53
2.4.4	Tracing the Identity of a Money Launderer	56
2.5	Making Use of the New (Web 2.0) Participatory Tools	59
2.5.1	Web 2.0 Initiatives	60
2.5.2	Discussion	60
2.6	Conclusion and Outlooks	61
	References	62
	Appendix: Table of FIDIS Web 2.0 Initiatives	66
VIGNETTE 2: VIRTUALLY LIVING IN VIRTUAL REALITIES		71
3	Virtual Persons and Identities	75
<i>David-Olivier Jaquet-Chiffelle, Emmanuel Benoist, Rolf Haenni, Florent Wenger, and Harald Zwingelberg</i>		
3.1	Modelling New Forms of Identities	76
3.1.1	Partial Identities and Virtual Identities	77
3.1.2	The Case of Legal Persons	78
3.1.3	Identity and Privacy Issues	79
3.1.4	Unifying Model Based on Virtual Persons	80
3.1.5	Illustration of Our Model	83
3.1.6	Conclusion	84
3.2	Pseudonyms in the Light of Virtual Persons	85
3.2.1	Johnny Hallyday	88
3.2.2	Conclusion	91
3.3	Virtual Persons and the Law	92
3.3.1	Unborn Human Entities	92
3.3.2	New Challenges to Technology and Law	95
3.3.3	Conclusion	97
3.4	Trust in the Light of Virtual Persons	97
3.4.1	Research on Trust	98
3.4.2	Defining Trust	100
3.4.3	Trust Metrics and Trust Management Systems	111
3.4.4	Trust in the Light of Virtual Persons	115
3.4.5	Conclusion	116
	References	117

VIGNETTE 3: USE AND ABUSE OF BIOMETRIC DATA AND SOCIAL NETWORKS 123

4 High-Tech ID and Emerging Technologies 129

Martin Meints and Mark Gasson

4.1	Identity Management and Identity Management Systems	130
4.2	Technologies and Technical Components	133
4.2.1	Public Key Infrastructure	133
4.2.2	Electronic Signatures	136
4.2.3	Biometrics	138
4.2.4	RFID	149
4.2.5	Credential Systems	154
4.3	Supporting Technologies	158
4.3.1	Trusted Computing	158
4.3.2	Protocols with Respect to Identity and Identification	162
4.3.3	Identity Management in Service Oriented Architectures	167
4.3.4	Digital Rights Management	171
4.4	Emerging Technologies	172
4.4.1	Ambient Intelligence	173
4.4.2	Human ICT Implants	175
4.5	Use Cases	176
4.5.1	ID Documents	176
4.5.2	CardSpace	181
4.6	Summary and Conclusions	183
	References	185

VIGNETTE 4: POWERING THE PROFILE: PLUGGING INTO THE MOBILE GRID 191

5 Mobility and Identity 195

Denis Royer, André Deuker, and Kai Rannenberg

5.1	GSM – How Mobile Communication Achieved Its Special Role in Identity Management	196
5.2	Mobile Identities – Context Added	198
5.2.1	Context Extension via LBS and User Control	198
5.2.2	Mobile Identities in Action – A Scenario on Emergency Response	200
5.3	The FIDIS Perspectives on Mobility and Identity	202

5.4	Technological Aspects	202
5.4.1	Management of Mobile Identities vs. Mobile Identity Management	203
5.4.2	Positioning Technologies and Methods	204
5.4.3	Accuracy of Positioning Technologies and Methods	211
5.4.4	Security and Privacy in Mobile Identity Management	211
5.5	Legal Aspects	215
5.5.1	Two European Directives on Data Protection	216
5.5.2	Location Data, Traffic Data, and Their Relation to Personal Data	217
5.5.3	Which Directives Apply to Which Types of Data?	219
5.5.4	Conclusion	220
5.6	Sociological Aspects	221
5.6.1	A Socio-technical View on Mobility and Identity	221
5.6.2	Price of Convenience (PoC)	223
5.7	Economic Aspects	225
5.7.1	Market Players	226
5.7.2	Building User Trust	227
5.7.3	Related Economic Theories	230
5.7.4	A Framework for Analysing the Economic Impacts of MIdM in Mobile Services and Applications	233
5.8	Requirements for Mobile Identity Management Systems	237
5.9	Outlook and Further Challenges and Questions	238
	References	240

VIGNETTE 5: HUMAN ENHANCEMENT, ROBOTS, AND THE FIGHT FOR HUMAN RIGHTS **243**

6 Approaching Interoperability for Identity Management Systems **245**

James Backhouse and Ruth Halperin

6.1	Introduction	245
6.1.1	Why Interoperability in iDMS: Relevance and Strategic Motivation	245
6.1.2	Interoperable Delivery of European eGovernment Services IDABC	246
6.1.3	Organization of This Chapter	247
6.2	Interoperable Identity Management Systems: Definitions and Framework	247

6.2.1	Conceptualizing Interoperability	247
6.2.2	The TFI Model	250
6.3	Stakeholders Perspectives on Interoperable iDMS	254
6.3.1	Expert Requirements for Interoperability	254
6.3.2	Citizens Perceptions on Interoperability	258
6.4	Conclusion	265
	References	265
	Appendix: Experts	267

VIGNETTE 6: MORE CONTROL FOR THE MACHINES 269

7 Profiling and Aml 273

Mireille Hildebrandt

7.1	Profiling: Definitions, Applications and Risks	275
7.1.1	What Is Profiling?	275
7.1.2	Applications of Profiling	278
7.1.3	Profiling, Democracy and the Rule of Law	283
7.2	Profiling Technologies as the Enabling Technology for Aml	286
7.2.1	What about Ambient Intelligence?	286
7.2.2	AmI and Autonomic Profiling	287
7.2.3	Autonomic Profiling and Autonomous Action	288
7.2.4	AmI, Democracy and Rule of Law	290
7.3	When <i>Idem</i> Meets <i>Ipse</i> : The Identity of the European Citizen	292
7.3.1	Privacy and Identity	292
7.3.2	Idem (Sameness) and Ipse (Selfhood)	293
7.3.3	Freedom from and Freedom to	294
7.4	A Vision of Ambient Law	295
7.4.1	AmLaw as Law	296
7.4.2	Why Should AmI Require Another Type of Law?	296
7.4.3	From Written to Digital Law in Constitutional Democracy	300
7.4.4	Legal and Technological PETs and TETs	302
7.5	Conclusions	305
	References	307

VIGNETTE 7: THE ROLE OF FORENSICS IN IDENTITY 311**8 Identity-Related Crime and Forensics 315***Bert-Jaap Koops and Zeno Geradts*

8.1	Introduction	315
8.2	Identity-Related Crime	316
8.2.1	The FIDIS Taxonomy of Identity-Related Crime	316
8.2.2	Aspects of Identity-Related Crime	322
8.3	Forensic Implications	329
8.3.1	Forensic Aspects	329
8.3.2	Example 1: Mobile Networks	331
8.3.3	Example 2: Biometric Devices	331
8.3.4	Conclusion	332
8.4	Forensic Profiling	333
8.4.1	Introduction	333
8.4.2	Definition of Forensic Profiling	334
8.4.3	Linkage Blindness and Limits of Profiling	334
8.4.4	Data Available	336
8.4.5	Structuring Evidence and Profiling	337
8.4.6	Forensic Profiling in an Investigative Perspective	337
8.4.7	Illicit Drug Profiling	341
8.4.8	Legal Aspects	342
8.5	Conclusion	344
	Reference	345

VIGNETTE 8: DATING 349**9 Privacy and Identity 351***Maike Gilliot, Vashek Matyas, and Sven Wohlgemuth*

9.1	Introduction	351
9.2	Privacy Aware Concepts for ID Numbers	353
9.2.1	Legal Aspects	354
9.2.2	Sociological Aspects	357
9.2.3	Technical Aspects	359
9.2.4	European Approaches	359
9.2.5	Conclusions	360
9.3	Privacy Primitives and Applications	362
9.3.1	Privacy Primitives	362
9.3.2	Application Privacy	365
9.3.3	Summary	372

9.4	Privacy with Delegation of Personal Data	372
9.4.1	The One-Sided Trust Model in CRM	373
9.4.2	Delegation of Rights in CRM	374
9.4.3	Security Systems and Delegation of Rights	376
9.4.4	DREISAM: Protocols for Delegation of Rights	378
9.4.5	Proof-of-Concept Implementation of DREISAM for CRM	381
9.4.6	Properties of DREISAM	383
9.4.7	Conclusion	385
9.5	Towards Transparency	385
	References	386

10 Open Challenges – Towards the (Not So Distant) Future of Identity **391**

Kai Rannenberg and Denis Royer

10.1	Identity Reference Architectures	391
10.1.1	What Is to Be Done?	392
10.1.2	How Can It Be Done?	392
10.1.3	What Needs to Be Considered?	393
10.2	Identity Management and Privacy	393
10.2.1	What Is to Be Done?	393
10.2.2	How Can It Be Done?	395
10.2.3	What Needs to Be Considered?	396
10.3	Identity Management and Multilateral Security	396
10.3.1	What Is to Be Done?	397
10.3.2	How Can It Be Done?	397
10.3.3	What Needs to Be Considered?	397
10.4	Identity in the Internet of Things	398
10.4.1	What Needs to Be Done?	398
10.4.2	How Can It Be Done?	398
10.4.3	What Needs to Be Considered?	398

Appendix A. List of Deliverables **401**

A.1	Communication Infrastructure (WP1)	401
A.2	Taxonomy: Identity of Identity (WP2)	402
A.3	HighTechID: Technologies to Support Identity and Identification (WP3)	404
A.4	Interoperability of Identity and Identification Concepts (WP4)	409
A.5	ID-Theft, Privacy and Security (WP5)	414

A.6 Forensic Implications (WP6)	417
A.7 Profiling (WP7)	418
A.8 Integration of the NoE (WP8)	422
A.9 Mobility and Identity (WP11)	423
A.10 Emerging Technologies (WP12)	425
A.11 Privacy Fundamentals (WP13)	427
A.12 Privacy in Business Processes (WP14)	430
A.13 eGovernment (WP16)	432
A.14 Abstract Persons (WP17)	432
Appendix B. Contributors	435
Appendix C. FIDIS Consortium	457
Appendix D. Proposal for a Common Identity Framework: A User-Centric Identity Metasystem	477
<i>Kim Cameron, Reinhard Posch, and Kai Rannenberg</i>	
D.1 Introduction	477
D.2 Terminology	477
D.3 Scope	480
D.4 Metasystem Requirements in the Light of Multilateral Security	480
D.5 Abstract Model of the Identity Metasystem	485
D.6 Enabling Technologies	495
D.7 Administration	498
D.8 Standardisation	499
Glossary	501