Lecture Notes in Computer Science 6545

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max Planck Institute for Informatics, Saarbruecken, Germany

Jan Camenisch Ronald Leenes Dieter Sommer
(Eds.)

Digital Privacy

PRIME – Privacy and Identity Management
for Europe

Springer

Volume Editors

Jan Camenisch
Dieter Sommer
IBM Research
Säumerstr. 4, 8803 Rüschlikon, Switzerland
E-mail: {jca, dso}@zurich.ibm.com

Ronald Leenes
Universiteit van Tilburg
TILT - Centrum voor Recht, Technologie en Samenleving
Postbus 90153, 5000 LE Tilburg, The Netherlands
E-mail: r.e.leenes@uvt.nl

Photos used for the front page design have been made by Christoph Edelhoff and licensed by PRIME consortium partner Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-19049-0 e-ISBN 978-3-642-19050-6
DOI 10.1007/978-3-642-19050-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011923224

CR Subject Classification (1998): K.4.1, K.4.4, K.6.5, D.4.6, E.3, H.2.0, H.3.5, C.2.0, C.2.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011
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, re-use of illustrations, recitation, broadcasting, reproduction on microfilms 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 permission for use must always be obtained from Springer. Violations are liable to 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.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

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

Foreword

During the past decade the digital society has firmly established itself in Europe and in many other parts of the world. Information and communication technology has emerged as the mission-critical backbone of modern economic and social life in the early 21st century. The contours of the dawning digital age have taken shape, and they include massive amounts of data, personal and non-personal, being continually generated and ceaselessly processed, exchanged, recombined, and often stored for indefinite periods of time. In this context, the creation of an electronic identity management infrastructure that puts the management of digital identity data under the users' control has manifested itself as one of the central challenges for life in the digital age.

The Internet transcends geographic and jurisdictional borders; hence there is a strong need for a global approach to trust in the digital society. Citizens look for value in the activities they do on the Internet. They want to be able to trust the technology and services provided and the actors behind. To forge a just and dignified digital future, and considering that trust is subjective and depends on context and culture, we need digital means, tools and instruments to allow us to sense the variables and reach a conclusion on the trustworthiness of services and third parties prior to engaging in interactions. To contribute to meeting these demands of the new age, trust, and with it identity management and privacy protection, are prominent elements of the ICT Research and Development Framework Programme of the European Union.

A flourishing digital society expects diversity, usability and openness, interoperability and competition as key drivers for trust and security. Diversity reduces the risks coming with dependence on one type of technology, and open standards and interoperability are key to competition, to empowering users to choose among a variety of products and services, and to the creation of business opportunities for small, medium and large companies alike.

PRIME – the 2008 recipient of the internationally renowned IAPP award for the best contribution to innovative privacy technology – has put Europe on the global map as a place for high-quality research on privacy. It has

effectively contributed to the preparation of Europe for a new digital age, for a digital life that preserves the shared European values of democracy, freedom and civil liberties. We would like to thank the PRIME project and all its partners for this 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.

December 2010

Jacques Bus (Head of Unit)
Dirk van Rooy (Head of Sector)
DG Information Society and Media
European Commission

Preface

Information technologies are becoming pervasive and powerful to the point that the privacy of citizens is now at risk. Indeed, more and more of our daily transactions are conducted electronically and require us to transmit personal information. Examples include using an electronic identity card to prove one's age in a bar, buying digital content on the Internet, checking our healthcare records on-line, or planning our next vacation. In this new information society, individuals need to be able to keep their autonomy and to retain control over their personal information, irrespective of their activities. The widening gap between this vision and current practices on electronic information networks undermines individuals' trust and threatens critical domains like mobility, healthcare, and the exercise of democracy.

Why Privacy and Identity Management

Closing this gap requires an identity management system that puts the users in control of their data and allows them to protect their privacy in electronic transactions. Indeed, we all manage our personal information (and thereby our identities) in our daily lives. However, the way we have learnt to do so for our non-electronic lives works poorly in the electronic society now taking shape for a number of reasons. First, we are often not aware what data about ourselves we are revealing in a transaction or we might even not be aware of the fact that we are revealing data to start with (e.g., making a call with a mobile phone reveals all kinds of (unexpected) data to unexpected parties). Second, the sheer complexity of the applications and their building blocks makes it almost impossible to understand where our data flows. Third, even if we were capable and willing to manage our electronic personal data and identities and protect our privacy, we would usually not be able to do so because the applications don't allow us to do so due to the way they are built. A well-known example is that users were asked for their social security number just so that the application could use it as a unique identifier.

PRIME's Solution

We, the PRIME partners, noted that the state of the art in privacy-enhancing mechanisms provides the technical means to build such a privacy-enhancing user-centric identity management system that would empower the users to manage their identity and protect their privacy. Thus the PRIME consortium was formed to prove this and to raise the awareness for privacy issues and their solutions. We chose an integrated approach to the legal, social, economic, and technical areas of concern to research, develop, and evaluate solutions to privacy-enhancing user-centric identity management. During the course of the project, we have developed a framework that integrates all technical and non-technical aspects of privacy-enhancing identity management and shows how privacy-enhancing technologies can be employed to realize privacy-enhancing user-centric identity management. We have elicited detailed requirements from legal, social, economic, and applicational points of view and have shown how they can be addressed, i.e., how to enable the users to effectively control their private sphere. That is, we have put forth an architecture that orchestrates the different privacy-enhancing technologies, including the human-computer interface. Based on this architecture, we have built several prototypes that exemplify privacy-enhancing user-centric identity management for a few selected application domains. We have validated our results by conducting experiments with end-users in these application areas. Moreover, we have considerably advanced the state of the art to address foundational technology, through research on human-computer interface, ontologies, authorization and cryptology, anonymous communications, and privacy-enhancing identity management systems architecture and assurance methods.

This Book

This book reports on the findings of the PRIME project. It is partitioned into five parts. The first part is a summary. It explains the privacy issues based on the example of Alice who goes shopping in the Internet. It then explains how PRIME resolves these issues. The second part of the book provides the legal, social, and economic landscape of privacy-enhancing identity management and derives requirements for privacy-enhancing user-centric identity management. The third part explains how privacy-enhancing user-centric identity management can be realized. It first describes the PRIME architecture which brings together the different privacy-enhancing mechanisms. These mechanisms are then subsequently explained. That is, we not only describe the results that the project has obtained based on these mechanisms, but also give a comprehensive overview of these technologies. The fourth part reports on how the PRIME architecture can be applied to applications. It describes the application prototypes that we have implemented and the lessons

we have learnt. This part further summarized the requirements on privacy-enhancing user-centric identity management in general and how they can be addressed. The fifth part features the conclusions we have drawn, provides an outlook to the future of trust, privacy and identity management, highlights open problems, and describes PRIME's follow-on projects.

More details for the results covered in this book as well as additional materials are available on the PRIME website www.prime-project.eu. The next page contains an overview of these materials.

July 2008

Jan Camenisch
Ronald Leenes
Dieter Sommer

Available PRIME Materials

The following materials are available on www.prime-project.eu:

Introductory Documents:

- Press releases, leaflets, and slide presentations outline the project objectives, approach, and expected results;
- The PRIME White Paper introduces privacy-enhancing identity management issues and PRIME's vision, solutions, and strategies;
- A number of tutorials introduce major concepts of privacy-enhancing identity management for use by the software development community and the general public.

PRIME Technical Materials:

- PRIME Framework reviews privacy-enhancing identity management issues; PRIME legal, social, and economic requirements; PRIME concepts and models; and PRIME architecture outlines.
- PRIME Requirements analyze in depth the legal, social, economic, and application requirements. They comprise generic requirements, as well as specific, scenario-based requirements of selected application areas including eLearning, location-based services, and airport security controls.
- PRIME Architecture describes in depth the organization and orchestration of the different privacy-enhancing technologies in a coherent PRIME system.
- Annual Research Reports review the research results gained in PRIME in each of the four years, and the research agenda for the subsequent years.
- HCI Guidance provides a comprehensive analysis of the Human-Computer Interface requirements and solutions for privacy-enhancing identity management.
- Assurance Methods survey the existing assurance methods that are relevant to privacy-enhancing identity management.
- Evaluation of Prototypes assesses a series of early PRIME technology prototypes from legal, social, and economic standpoints.
- More than 200 scientific publications address results produced in all PRIME-related fields within the scope of the project. The abstracts of those papers and links to them are listed in the four Annual Research Reports which are available from PRIME's website www.prime-project.eu.

Project Partners

The PRIME Project was undertaken by the following 22 partners.

Compagnie IBM France	France
International Business Machines of Belgium	Belgium
IBM Research GmbH	Switzerland
Unabhängiges Landeszentrum für Datenschutz	Germany
Technische Universität Dresden	Germany
Deutsche Lufthansa AG	Germany
Katholieke Universiteit Leuven	Belgium
T-Mobile International AG	Germany
Hewlett-Packard Ltd.	UK
Karlstads Universitet	Sweden
Università degli Studi di Milano	Italy
Joint Research Centre	Italy
Centre National de la Recherche Scientifique	France
Johann Wolfgang Goethe Universität Frankfurt	Germany
Chaum LLC	USA
Rheinisch-Westfälische Technische Hochschule Aachen	Germany
Institut EURECOM	France
Erasmus Universiteit Rotterdam	The Netherlands
JaTeK GmbH	Germany
Universiteit van Tilburg	The Netherlands
Fondazione Centro San Raffaele del Monte Tabor	Italy
Swisscom AG	Switzerland

Of these partners, JaTeK left the consortium shortly after the project had started as the company dissolved, IBM France was replaced by IBM Belgium because of the change of the project coordinator, and Institut EURECOM left in the third project year because of key persons leaving the institution.

Contributors to PRIME

The following people contributed to the PRIME Project.

Gérard Lacoste from IBM France; Eric Goderniaux from IBM Belgium; Endre Bangerter, Anthony Bussani, Jan Camenisch, Günter Karjoth, Susan Hohenberger, Abhi Shelat, Dieter Sommer, Michael Waidner, and Roger Zimmermann from IBM Research; Marit Hansen, Marita Häuser, Henry Krasemann, Christian Krause, Jan Möller, Antje Nageler, Maren Raguse, Martin Rost, Jan Schallaböck, and Harald Zwingelberg from Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein; René Balzer, Mike Bergmann, Stefan Berthold, Katrin Borcea-Pfitzmann, Rainer Böhme, Alexander Böttcher, Sebastian Clauß, Hilko Donker, Elke Franz, Andreas Juschka, Benjamin Kellermann, Thomas Kriegelstein, Katja Liesebach, Andreas Pfitzmann, Stefanie Pötzsch, Immanuel Scholz, Stefan Schiffner, Anne-Katrin

Stange, Sandra Steinbrecher, and Hagen Wahrig from Technische Universität Dresden; Jean-Marie Willigens from Lufthansa; Anna Buchta, George Danezis, Claudia Díaz, Jos Dumortier, Markulf Kohlweiss, Eleni Kosta, Klaus Kursawe, Gregory Neven, Len Sassaman, Michaël Vanfleteren, and Karel Wouters from KU Leuven; Pete Bramhall, Marco Casassa Mont, Stephen Crane, Siani Pearson, Annie Chan, Tariq Elahi, Filipe Beato, Amadeu Santos, Damien Allison, Daniel Gray, and Daniel Drozdzewski from HP Labs; Christer Andersson, Camilla Carlander, Ninni Danielsson, Hans Hedbom, Simone Fischer-Hübner, Maria Lindström, Leonardo Martucci, Jenny Nilsson, John-Sören Pettersson, Nina Rönntorp, and Albin Zuccato from Karlstad University; Claudio A. Ardagna, Alberto Colombo, Marco Cremonini, Ernesto Damiani, Sabrina De Capitani di Vimercati, Cristiano Fugazza, Eros Pedrini, and Pierangela Samarati from Università degli Studi di Milano; Sami Dufva, Giles Hogben, Jan Löschner, Neil Mitchison, Zdenek Riha, Guenter Schumacher, Ioannis Vakalis, and Marc Wilikens from JRC; Anas Abou El Kalam, Carlos Aguilar Melchor, Jean Arlat, Yves Deswarte, Vincent Nicomette, David Powell, Matthieu Roy, Frédéric Sorbet, Boris Valera, and Christophe Zanon from LAAS-CNRS; Lothar Fritsch, Christian Kahl, Markulf Kohlweiss, Mike Radmacher, Kai Rannenberg, Tobias Scherner, and Jan Zibuschka from Goethe University Frankfurt; David Chaum from Chaum LLC; Dogan Kesdogan, Andriy Panchenko, and Lexi Pimenidis from RWTH Aachen University; Walid Bagga, Stefano Crosta, and Refik Molva from Eurecom; Marcel van Oosterhout, Louis-Francois Pau, and Jimmy Tseng from Erasmus University Rotterdam; Robbert-Jan Dijkman, Alea Fairchild, Ronald Leenes, Isabelle Oomen, Bart Priem, Marcel Hoogwout, Rachel Marbus, Mirjam Lips, Kees Lune, Simone van der Hof, Caroline Franke, and Piet Ribbers from Tilburg University; Marco Bianchi, Simone Feriti, Vadla Pavan Kumar, Nicola Maganetti, Alberto Sanna, and Ricardo Serafin Fondazione Centro San Raffaele del Monte Tabor; Peter Keller from Swisscom; Marc Wilhelm, Tobias Kölsch, and Georg Kramer from T-Mobile; John Borking from Borking Consulting; Thomas Roessler and Rigo Wenning from W3C; and Ronald F. Koorn from KPMG IT Advisory.

Acknowledgements

Throughout the four years we conducted the project, we had the pleasure of discussing the topic of privacy and identity management with lots of interesting people. In particular, we are most grateful to the following persons who enabled us to reach and exceed our goals: Dimitris Antoniadis, Giuseppe Ateniese, Michael Backes, Mira Belenkiy, Abhilasha Bhargav-Spantzel, Cesar Castrat, Petros Cheretakis, Melissa Chase, Alain Esterle, Christian Feig, Fernando Galindo, Marco Geißler, Thomas Gross, Jens Groth, Evert-Jan de Jongste, Jens Kempe, George Kontaxis, Alexander Hahn, Tom Heydt-Benjamin, Sebastian Höhne, Håkan K. Kvarnström, Maciej Koprowski, Alexander Lemke, Anna Lysysankaya, Evangelos Markatos, Breno

de Medeiros, Martin Meinhold, Anton Mityagin, Tony Nadalin, Michael Østergaard Pederson, Peter Pfeifhofer, Michalis Polychronakis, Federico Puccioni, Mema Roussopoulos, Claudio Soriente, Patrick Symmangk, Luc Taal, Jeroen Terstegge, Frank Tewari, Raymond Tsai, and Bogdan Warinschi.

The official project reviews helped us to stay on track and critically examine our achievements. A big thank you therefore goes to our reviewers Alberto Escudero Pascual, Nathalie Weiler, and Louise Yngström, as well as to our project officers Alain Jaume, Richard Sonnenschein, Günter Schumacher, and Dirk van Rooy.

Finally, we are most grateful to the members of the PRIME Reference Group who discussed the project with us in three meetings and via e-mail: Emilio Aced Felez, Bruno Baeriswyl, Emilie Barrau, Ruud Beugelsdijk, Caspar Bowden, Ian Brown, Johann Čas, Malcolm Crompton, Tessa van Dorp, Boris Erdmann, Esther Hefti, Giles Hogben, Waltraut Kotschy, Christopher Kuner, Cornelia Kutterer, Yann LeHegarat, Helena Lind, Francisco José López Carmona, Ludwig Oberendorff, Peter Schaar, Peter Sommer, Vincent Tilman, and Luk Vervenne.

Contents

Part I: Privacy and Identity Management

1 An Introduction to Privacy-Enhancing Identity Management . . . 3
Jan Camenisch, Ronald Leenes, Marit Hansen, and Jan Schallaböck
1.1 Motivation . . . 4
1.2 A Scenario – Alice Goes Shopping . . . 6
1.3 PRIME Enabled Shopping . . . 7
1.3.1 Phase 1: Buyer Beware . . . 8
1.3.2 Phase 2: Pre-sales – Starting from Maximum Privacy . . . 9
1.3.3 Phase 3: Ordering – Informed Consent and Purpose Limitation . . . 10
1.3.4 Phase 4: After-Sales and Delivery – Retaining Control: Policy Enforcement . . . 13
1.3.5 Phase 5: Customer Relationship – Building the Relationship . . . 14
1.3.6 Phase 6: Beyond Being a Connoisseur – Alice's Other Identities . . . 15
1.4 The Bigger Picture . . . 17
1.4.1 Concepts and Human-Computer Interaction . . . 18
1.4.2 Public Awareness . . . 18
1.4.3 Economics . . . 19
1.4.4 Reaching Out . . . 20
1.5 Requirements for Identity Management Systems . . . 20

References . . . 23

Part II: Setting the Stage

2 Overview and Introduction Part II . . . 27
Ronald Leenes
2.1 Introduction . . . 27
2.2 An Approach From Three Perspectives . . . 29
2.3 Structure Part II . . . 30

3 The Identity Landscape 33
Bart Priem, Ronald Leenes, Eleni Kosta, and Aleksandra Kuczerawy
3.1 Introduction 33
3.2 The Concept of (Online) Identity 34
3.3 Asymmetric Perspectives 35
3.3.1 The Enterprise-Centric View on Identity Management 35
3.3.2 A User-Centric View on Identity Management 36
3.3.3 Combining the Perspectives 37
3.4 Evolving Identity Management Systems 38
3.5 Existing Identity Management Applications 40
3.5.1 Microsoft Passport 40
3.5.2 Liberty Alliance 41
3.5.3 OpenID 42
3.5.4 Microsoft Cardspace 42
3.5.5 Other IdM Systems 43
3.6 Complicating the Online Identity Landscape 43
3.6.1 The Internet as a Social Environment 44
3.6.2 Customer Empowerment 44
3.6.3 Identity-Related Crime and Misbehaviour 45
3.6.4 The Expanding Internet: Always-On and Everywhere 46
3.6.5 The Internet of Things and the Citizens of Tomorrow 47
3.6.6 Identifying the Individual in the Era of the Internet of Things 48
3.7 Conclusion 50

4 The Need for Privacy-Enhancing Identity Management 53
Bart Priem, Ronald Leenes, Alea Fairchild, and Eleni Kosta
4.1 Introduction 53
4.2 Individual Perspective 54
4.2.1 Power Imbalance 55
4.2.2 Relations 57
4.2.3 Personal Development 58
4.2.4 Behaviour, Health, and Emotions 59
4.3 Organisational Perspective 60
4.3.1 Business 60
4.3.2 Government Services 63
4.4 Societal Perspective 64
4.4.1 The Determination of Privacy in Social Context 65
4.4.2 The Contribution of Privacy-Enhanced IdM to Society 66
4.5 Conclusion 70

5 Regulating Identity Management 73
Eleni Kosta, Aleksandra Kuczerawy, Ronald Leenes, and Jos Dumortier
5.1 Introduction 73
5.2 A Brief History of European Data Protection Regulation ... 74
5.2.1 The EU Data Protection Directive 76
5.2.2 The ePrivacy Directive 78
5.2.3 Other Relevant Directives 79
5.3 Principles of Data Processing 79
5.3.1 Principles on Processing of Personal Data 80
5.3.2 Rights of the Data Subject 83
5.3.3 Specific Requirements for Electronic Communications Systems or Applications 85
5.4 Applicability Issues of the Current Legal Framework 86
5.4.1 An Old Directive for New Technologies 86
5.4.2 The Role of the ePrivacy Directive with Regard to the Challenges Posed by New Technologies 87
5.5 Conclusion 89

6 User-Centric Privacy-Enhancing Identity Management 91
Bart Priem, Eleni Kosta, Aleksandra Kuczerawy, Jos Dumortier, and Ronald Leenes
6.1 Introduction 91
6.2 Sources of the User-Perspective Requirements 92
6.2.1 Audience Segregation 92
6.2.2 User Control 94
6.2.3 Adoption of Privacy-Enhanced IdM in Society 102
6.3 Conclusions 105

7 Privacy-Enhancing Identity Management in Business 107
Alea Fairchild and Piet Ribbers
7.1 Introduction 107
7.2 Business Model for Privacy Enhancement 108
7.2.1 Privacy Adoption Drivers 108
7.2.2 Process Maturity for Privacy 113
7.2.3 Risk Analysis for Data Privacy 120
7.2.4 Privacy Impact on Business Process Design 122
7.3 Cost Benefit Analysis of Privacy 124
7.4 Requirements from a Business Perspective 127
7.5 Conclusion 129

References 131

Part III: What Technology Can Do for Privacy and How

8 Introduction: Privacy, Trust, and Identity Management . . . 141
Stephen Crane, Siani Pearson, and Dieter Sommer
8.1 Trust . . . 142
8.1.1 Analysis of Trust . . . 143
8.1.2 Establishing Trust and Managing Privacy . . . 144
8.1.3 Understanding Trust . . . 144
8.2 Structure . . . 147

9 Architecture . . . 151
Dieter Sommer
9.1 Introduction . . . 151
9.1.1 Motivation and Goals . . . 151
9.1.2 Realizing the Goals: Technology . . . 153
9.1.3 Related Work . . . 156
9.1.4 Outline . . . 158
9.2 Architecture Overview . . . 158
9.2.1 One Party in the System . . . 158
9.2.2 Parties and Interactions . . . 159
9.2.3 Data . . . 163
9.2.4 Components . . . 170
9.3 Data Model . . . 173
9.3.1 Identity . . . 174
9.3.2 Constants . . . 176
9.3.3 Formulae in First-Order Logic . . . 176
9.3.4 Predicates . . . 177
9.3.5 Connectives . . . 177
9.3.6 Subject . . . 178
9.3.7 Identifier Objects . . . 179
9.3.8 Certification Metadata . . . 181
9.3.9 Conditional Release . . . 182
9.3.10 Anonymity Revocation . . . 184
9.3.11 Typing . . . 184
9.3.12 Automated Reasoning . . . 188
9.3.13 Requests of Data . . . 191
9.3.14 Matching Data against Requests . . . 194
9.3.15 Further Discussion . . . 196
9.4 Data Representation Based on Our Model . . . 199
9.4.1 Identifier Relationships . . . 200
9.4.2 Identity Relationships . . . 201
9.4.3 Data Track . . . 206
9.4.4 Profile Data . . . 208

9.4.5 Data Statements and Requests 209
9.5 Identity Management Concepts 210
9.5.1 Partial Identities 210
9.6 Data Exchange Architecture 212
9.6.1 Roles in an Attribute Exchange Scenario 214
9.6.2 Private Certificate Systems 215
9.6.3 High-Level Architecture 216
9.6.4 Component Interface 217
9.6.5 Components 234
9.6.6 Aspects of System Architecture 237
9.7 Authorization Policies 242
9.7.1 Paradigms of Authorization Systems 242
9.7.2 Our Approach 243
9.7.3 Language Basics 244
9.7.4 Language Extensions 245
9.7.5 Rule Composition 251
9.7.6 Associating Policies with Resources 252
9.7.7 Architectural Integration 258
9.8 Data Handling Policies 260
9.8.1 Model 260
9.8.2 Association of Policies with Data 264
9.8.3 Policy Negotiation 267
9.8.4 Concrete Realization in the PRIME Prototype 270
9.9 Negotiation – Exchange of Data 271
9.9.1 Overview 272
9.9.2 Negotiation Model 274
9.9.3 Policy-Driven Negotiation 276
9.9.4 A Round of Negotiation 277
9.10 Conclusions 285
9.10.1 Key Contributions 285
9.10.2 Experience 286

10 Pseudonyms and Private Credentials 289
Jan Camenisch, Markulf Kohlweiss, and Dieter Sommer
10.1 Introduction 289
10.2 The Idemix Private Credential System 290
10.2.1 Basic Principles of Strong Authentication 290
10.2.2 Balancing Anonymity and Accountability 291
10.3 The Idemix System 292
10.3.1 Required Properties When Showing a Certificate 292
10.3.2 Cryptographic Primitives 294
10.3.3 Cryptography for the Controlled Release of Certified Data 297
10.4 Building Applications Using Idemix 300
10.4.1 An Anonymous Credential System 300

10.4.2 Anonymity Revocation 302
10.4.3 Balancing Anonymity and Accountability Using e-Cash Techniques 303
10.4.4 Application Scenarios 305
10.5 Historical Notes 308

11 Privacy Models and Languages: Access Control and Data Handling Policies 309
Claudio Agostino Ardagna, Sabrina De Capitani di Vimercati, and Pierangela Samarati
11.1 Introduction 309
11.2 Privacy Policy Categories 310
11.3 Scenario 311
11.4 Access Control Model and Language 313
11.4.1 Basic Concepts 313
11.4.2 Functionalities 315
11.4.3 Description of the Access Control Language 316
11.5 Data Handling Model and Language 320
11.5.1 Description of the Data Handling Language 322
11.6 Related Work 326
11.7 Conclusions 329

12 Privacy Models and Languages: Obligation Policies 331
Marco Casassa Mont
12.1 Introduction to Privacy Obligation Policies 331
12.2 Analysis of Privacy Obligations 332
12.3 Requirements and Constraints 336
12.4 Model of Privacy Obligations 339
12.4.1 Conceptual View 340
12.4.2 Formal View 341
12.4.3 Operational View 342
12.4.4 Relationships with AC/DHP Policies 345
12.5 Privacy Obligation Policies: Language 346
12.6 Parametric Obligation Policies 352
12.6.1 Parametric Obligation Policies: Model 353
12.6.2 Parametric Obligation Policies: Reference Scenario . . . 355
12.6.3 Parametric Obligation Policies: Language 355
12.7 Discussion 361
12.8 Next Steps and Future R&D Work 361

13 Privacy Models and Languages: Assurance Checking Policies 363
Siani Pearson
13.1 Introduction 363
13.1.1 Principles 364

13.1.2 Natural Language Examples 364
13.1.3 Overview of Different Potential Approaches 365
13.2 Defining Trust Constraints: A Lower Level Representation 365
13.3 Defining Clauses as First Class Objects: A Higher-Level Representation 368
13.3.1 Conceptual View 368
13.3.2 Examples of Clauses 370
13.3.3 Formal View 371
13.3.4 Operational View 371
13.3.5 Representation of Assurance Policies in XML Format 372
13.4 Analysis 373
13.5 Next Steps and Future R&D Work 375

14 Privacy-Aware Access Control System: Evaluation and Decision 377
Claudio Agostino Ardagna, Sabrina De Capitani di Vimercati, Eros Pedrini, and Pierangela Samarati
14.1 Introduction 377
14.2 Interplay between Parties 379
14.3 A Privacy-Aware Access Control Architecture 381
14.3.1 Access Control Decision Function 381
14.3.2 Policy Management 383
14.4 Policy Evaluation 384
14.5 A Privacy-Aware Access Control System Prototype 385
14.5.1 ACDF Prototype 386
14.5.2 PM Prototype 388
14.6 Performance Analysis 389
14.6.1 The Evaluation Flow 390
14.6.2 Performance Results 391
14.7 Conclusions 394

15 Privacy-Aware Identity Lifecycle Management 397
Marco Casassa Mont
15.1 Privacy-Aware Identity Lifecycle Management: Principles and Concepts 397
15.1.1 Obligation Management Framework 397
15.2 Obligation Management System 399
15.2.1 Design Rationale 399
15.2.2 System Architecture 400
15.2.3 Implementation Details 404
15.2.4 Interaction Flow 411
15.2.5 Event Management Framework 413

15.2.6 Data Repository 414
15.2.7 Administration GUI 417
15.2.8 Discussion 421
15.3 Scalable Obligation Management System 421
15.3.1 Scalable Obligation Management Framework 421
15.3.2 System Architecture 423
15.4 Discussion and Conclusions 426

16 Privacy Assurance Checking 427
Siani Pearson and Tariq Elahi
16.1 Introduction 427
16.1.1 Scenarios Considered 429
16.1.2 How Assurance Checking Fits in with the PRIME Approach 430
16.1.3 Assurance Control Framework: Overview 432
16.2 Privacy Compliance Checking System 433
16.2.1 Design Rationale 433
16.2.2 Architecture 433
16.2.3 Key Interfaces 437
16.2.4 Implementation Details 441
16.2.5 Mapping and Capability Validation 443
16.2.6 Description of Protocol 445
16.2.7 Role of Third Parties within the Trust Chain 449
16.2.8 Extension to B2B Scenarios 451
16.3 Comparison with Related Work 452
16.4 Next Steps and Future R&D Work 455
16.5 Conclusions 455

17 Security/Trustworthiness Assessment of Platforms 457
Stephen Crane and Siani Pearson
17.1 Introduction 457
17.2 Assessment of Trust 457
17.2.1 Trust in an Organisation 458
17.2.2 Trust 459
17.2.3 Determining Trustworthiness 459
17.2.4 Summary 462
17.3 Assessing the Impact of Computer Systems in Relation to On-Line Trust 462
17.3.1 Analysis of Online Trust 462
17.3.2 How On-Line Trust Is Underpinned by Social and Technological Mechanisms 463
17.3.3 Summary 464
17.4 Deploying Trusted Technologies 465
17.4.1 Trusted Computing Technology 465

17.4.2 How Trusted Platforms Can Provide Persistent and Dynamic Trust . . . 466
17.4.3 Summary . . . 468
17.5 Use of Trusted Computing to Enhance Privacy . . . 469
17.5.1 Introduction . . . 469
17.5.2 How Trusted Computing Platform Technology Can Enhance Privacy . . . 469
17.5.3 Privacy Enhancing Safeguards of Trusted Computing Technology . . . 470
17.5.4 How Such Building Blocks Can Be Used . . . 472
17.5.5 Potential Negative Privacy Implications of Trusted Computing . . . 474
17.5.6 Concluding Remarks . . . 476
17.6 PRIME Platform Trust Manager (PTM) . . . 477
17.6.1 Trust Handler (TH) . . . 480
17.6.2 Trust Real-Time Monitor (TRM) . . . 480
17.6.3 Platform Trust Status (PTS) . . . 480
17.6.4 Trust Communicator (TC) . . . 481
17.6.5 Reputation Manager (RM) . . . 482
17.6.6 Trust Wrapper (TW) . . . 482
17.7 Reputation Management . . . 482
17.7.1 Objective Reputation Assessment . . . 482
17.7.2 Privacy Preferences and Privacy Obligations . . . 483
17.8 Conclusions . . . 483

18 Further Privacy Mechanisms . . . 485
Anas Abou El Kalam, Carlos Aguilar Melchor, Stefan Berthold, Jan Camenisch, Sebastian Clauß, Yves Deswarte, Markulf Kohlweiss, Andriy Panchenko, Lexi Pimenidis, and Matthieu Roy
18.1 Privacy Measures . . . 485
18.1.1 Formal Methods . . . 487
18.1.2 Persistent Data and Statistical Databases . . . 490
18.1.3 Data-Flow in Networks . . . 492
18.1.4 Generalizations . . . 494
18.2 Data Anonymization . . . 502
18.2.1 Introduction . . . 502
18.2.2 Analysis of Some Anonymization Examples in Europe and the USA . . . 504
18.2.3 Requirements for a Suitable Implementation . . . 510
18.2.4 A Generic Anonymization Architecture . . . 515
18.2.5 Implementation . . . 518
18.2.6 Discussion . . . 519
18.2.7 Conclusions . . . 520
18.3 Anonymous Communication . . . 521
18.3.1 Scenario . . . 522

18.3.2 Techniques and Approaches 526
18.3.3 Threats in Anonymous Communication 540
18.3.4 Legal Issues 543
18.4 Unobservable Content Access 543
18.4.1 Private Information Retrieval and Oblivious Transfer 545
18.4.2 Access Control for Unobservable Services 546
18.4.3 Location-Based Services 547
18.4.4 Conclusion and PRIME Perspective 555

19 Reputation Management as an Extension of Future Identity Management 557
Sandra Steinbrecher, Franziska Pingel, and Andreas Juschka
19.1 Introduction 557
19.2 Model of Reputation Systems 559
19.2.1 Reputation 559
19.2.2 Reputation Network 560
19.3 Reputation within BluES'n 563
19.3.1 Characteristics of a Reputation System in the Context of Collaborative eLearning 563
19.3.2 Basic Design of the Reputation System 563
19.4 Reputation as Service for PRIME Applications 565
19.4.1 Necessary Infrastructure 565
19.4.2 System Design 566
19.5 Outlook 568

20 Human-Computer Interaction 569
Simone Fischer-Hübner, John Sören Pettersson, Mike Bergmann, Marit Hansen, Siani Pearson, and Marco Casassa Mont
20.1 Introduction 569
20.2 Related Work 570
20.2.1 User-Friendly Representation of Policy Management with the Help of Default Settings 571
20.2.2 Secure Interfaces 571
20.2.3 Mapping Legal Privacy Requirements 572
20.2.4 Mediation of Trust 573
20.3 Challenge I: User-Friendly Representation of Complex PET Concepts 573
20.3.1 Simplified Policy Handling 574
20.3.2 UI Paradigms for Presenting Privacy Preferences 577
20.4 Challenge II: Secure Interfaces 581
20.5 Challenge III: Mapping Legal Privacy Requirements 582
20.5.1 Obtaining Informed Consent 582
20.5.2 Enhancing Transparency 587

20.6 Challenge IV: Mediation of Trust 591
20.7 Outlook 593
20.7.1 Disclosing Data Using Anonymous Credentials 593
20.7.2 Notification about Incidents 593
20.7.3 Linkability Computation 594
20.7.4 How Ontologies Can Be Utilised for UI Design 594

21 Technology Assurance 597
Tobias Scherner and Lothar Fritsch
21.1 Introduction 597
21.1.1 Cost of Testing 598
21.1.2 Common Criteria 599
21.2 Early Security Validation with CC 599
21.2.1 Evaluation and the Common Criteria 599
21.2.2 Basic Preconditions for an Evaluation 600
21.2.3 Implemented Security Functions 601
21.2.4 Threat Analysis 601
21.2.5 Test Plans 602
21.2.6 The Documentation of the Test Results 603
21.2.7 Evaluation Process 603
21.2.8 Experience with CC-Based Project Evaluation 604
21.2.9 Integrated Prototype 604
21.2.10 LBS Prototype 605
21.2.11 eLearning Prototype 605
21.3 Conclusion 607

22 Requirements for Identity Management from the Perspective of Multilateral Interactions 609
Stefanie Pötzsch, Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, and Sandra Steinbrecher
22.1 Introduction 609
22.1.1 Objective of the Chapter 609
22.1.2 User-Controlled Identity Management: From Chaum to PRIME 610
22.2 Multilateral Interactions Using the Example of a Collaborative eLearning System 611
22.2.1 Multilateral Interactions 611
22.2.2 Stakeholders 611
22.3 Building Blocks of a Privacy-Enhancing Identity Management System for MLI 613
22.3.1 Pseudonyms and Partial Identities 614
22.3.2 Relationship Information 614
22.3.3 Searching for and Finding of Interaction Partners 615
22.3.4 Trust Management and Reputation 616
22.3.5 Awareness Information 617

22.3.6 Context and History 617
22.3.7 Access Control 618
22.3.8 Negotiation and Enforcement of Privacy Policies and Preferences 619
22.3.9 Workflows and Behaviour Patterns 619
22.3.10 External Regulations 620
22.4 Summary and Outlook 621
22.4.1 Overview of Building Blocks 621
22.4.2 Building Blocks in the Model of David Chaum 622
22.4.3 Research Questions 623

References 627

Part IV: PRIME Applied

23 Introduction 653
Pete Bramhall

24 Collaborative E-Learning 657
Katja Liesebach, Elke Franz, Anne-Katrin Stange, Andreas Juschka, Katrin Borcea-Pfitzmann, Alexander Böttcher, and Hagen Wahrig
24.1 The Collaborative eLearning System BluES'n 657
24.1.1 Democratisation of an eLearning Environment 657
24.1.2 Need for Privacy and How PRIME Helps 659
24.2 Intra-Application Partitioning of Personal Data 661
24.2.1 Necessity and General Goals 661
24.2.2 Concept for the Support of IAP 662
24.2.3 Realisation within the CeL Prototype 663
24.2.4 Discussion 664
24.3 Policy- and Credential-Based Access Control 665
24.3.1 Necessity for Privacy-Enhancing Access Control 665
24.3.2 Realisation within the CeL Prototype 665
24.3.3 Discussion 666
24.4 Privacy-Aware and Usable Application Design 667
24.4.1 Management of Aliases 668
24.4.2 Chernoff Faces 669
24.4.3 GUI Components: InfoCenter and Echobar 671
24.4.4 Adapted "Send Personal Data"-Dialogue 672
24.5 Summary – The Final CeL Prototype 673
24.6 Beyond PRIME – An Outlook 676

25 Location-Based Services ... 679
Jan Zibuschka, Kai Rannenberg, and Tobias Kölsch
25.1 Introduction ... 679
25.2 Privacy in Location-Based Services ... 679
25.3 Requirements ... 681
25.3.1 Business Models ... 681
25.3.2 Data Protection ... 682
25.4 The Concept of a Location Intermediary ... 683
25.5 Prototype Development ... 685
25.6 PRIME Principles in a Restricted Mobile Environment ... 686
25.7 First Prototype Version ... 687
25.7.1 Scenario ... 687
25.7.2 Implementation ... 687
25.8 Second Prototype Version ... 690
25.8.1 Scenario ... 690
25.8.2 Implementation ... 690
25.9 Commercialization ... 692
25.10 Possible Deployment ... 693
25.11 Outlook ... 694

26 e-Health ... 697
Alberto Sanna, Riccardo Serafin, and Nicola Maganetti
26.1 Introduction ... 697
26.1.1 Definition of "Health" by the World Health Organization (WHO) ... 698
26.1.2 Continuity of Care and Impact on Individual's Life ... 698
26.1.3 Health and Lifestyle Management ... 699
26.1.4 The Self Care Medication Regimen and the Opportunity for Privacy-Enhanced Processes and Services ... 700
26.1.5 Reference Context for Privacy-Enhanced Process and Service Re-engineering Based on the PRIME Concepts Applied to Self Care Drug Therapy Management ... 706
26.2 A Healthcare Demonstrator: Objectives and Scenario ... 707
26.2.1 Objectives ... 707
26.2.2 Scenario ... 708
26.2.3 Collaboration with Other European Research Initiatives ... 710
26.3 Application Requirements ... 711
26.4 Application Demonstrator Architecture ... 713
26.4.1 Demonstrator Components ... 713

26.4.2 Privacy-Enhanced Online Drug Purchase: Information Flow . . . 713
26.4.3 Data Track and Obligations: Ensuring User Control . . . 717
26.5 Conclusion . . . 719

27 Airport Security Controls: Prototype Summary . . . 721
Ioannis Vakalis
27.1 Introduction . . . 721
27.2 The Reason Behind the Prototype . . . 722
27.3 The Trusted Traveler Use Case Scenario . . . 723
27.3.1 Privacy Enhancements . . . 724
27.4 Trusted Traveler "Smart Card" and Data Stored Therein . . . 724
27.5 The ASC Prototype Stages . . . 725
27.5.1 The Enrollment . . . 725
27.5.2 Check-In . . . 727
27.5.3 Entering the Passenger Restricted Area (PRA) . . . 729
27.5.4 Gate . . . 731
27.5.5 Boarding . . . 732
27.5.6 The Use of Cryptography . . . 733

28 Privacy and Identity Management Requirements: An Application Prototype Perspective . . . 735
Tobias Kölsch, Jan Zibuschka, and Kai Rannenberg
28.1 Introduction . . . 735
28.2 Users' Interests and Requirements . . . 736
28.2.1 Data Minimization . . . 736
28.2.2 Control of Data Flow . . . 739
28.2.3 Easy-to-Use Technology . . . 741
28.2.4 Reliable Service Provision . . . 742
28.3 Service Providers' Interests and Requirements . . . 742
28.3.1 Flexible Business Models . . . 743
28.3.2 Customer Loyalty and Trust . . . 743
28.3.3 User Base . . . 743
28.3.4 Trusted Payment Partners . . . 744
28.3.5 Delegation . . . 745
28.3.6 Legal Compliance . . . 745
28.4 Network Operators' Interests and Requirements . . . 745
28.4.1 Flexible Business Models . . . 746
28.4.2 Easy Integration of Third-Party Services . . . 746
28.4.3 Legal Compliance . . . 747
28.4.4 Customer Loyalty and Trust . . . 747
28.4.5 Leveraging Existing Infrastructural Assets . . . 747

28.4.6 Enabling New Applications 747
28.5 Developer Requirements 747
28.5.1 Documentation 747
28.5.2 Lean Interfaces 748
28.5.3 Integration into Existing Frameworks 748
28.6 Conclusion 748

References 751

Part V: Conclusion and Outlook

29 Conclusion and Outlook 759
Jan Camenisch and Andreas Pfitzmann
29.1 Conclusion 759
29.2 Outlook 760
29.2.1 Further Research on Identity Management 760
29.2.2 Making Privacy Real 761
29.2.3 Including the Social Value of Privacy 762
29.2.4 Succeeding PRIME 763

References 765

Part VI: Appendix

30 XML Schemata 769
30.1 Access Control and Release Language: XML Schema 769
30.2 Data Handling Language: XML Schema 771

Author Index 775