

Jan Camenisch Ronald Leenes Dieter Sommer
(Eds.)

Digital Privacy

PRIME - Privacy and Identity Management
for Europe

Springer

Contents

Part I: Privacy and Identity Management

1	An Introduction to Privacy-Enhancing Identity Management	3
	<i>Jan Camenisch, Ronald Leenes, Marit Hansen, and Jan Schallabock</i>	
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

	Overview and Introduction Part II	27
	<i>Ronald Leenes</i>	
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
	<i>Eleni Kosta, Aleksandra Kuczerawy,</i>	
	<i>Ronald Leenes, and Jos Dumortier</i>	
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
	<i>Bart Priem, Eleni Kosta, Aleksandra Kuczerawy,</i>	
	<i>Jos Dumortier, and Ronald Leenes</i>	
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
	<i>Alea Fairchild and Piet Ribbers</i>	
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

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

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
	<i>Claudio Agostino Ardagna, Sabrina De Capitani di Vimercati, and Pierangela Samarati</i>	
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
	<i>Marco Casassa Mont</i>	
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
	<i>Siani Pearson</i>	
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
	<i>Claudio Agostino Ardagna, Sabrina De Capitani di Vimercati, Eros Pedrini, and Pierangela Samarati</i>	
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
	<i>Marco Casassa Mont</i>	
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
	<i>Siani Pearson and Tariq Elahi</i>	
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
	<i>Stephen Crane and Siani Pearson</i>	
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
	<i>Anas Abou El Kalam, Carlos Aguilar Melchor, Stefan Berthold, Jan Camenisch, Sebastian Claufi, Yves Deswarte, Markulf Kohlweiss, Andriy Panchenko, Lexi Pimenidis, and Matthieu Roy</i>	
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
	<i>Sandra Steinbrecher, Franziska Pingel, and Andreas Juschka</i>	
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
	<i>Simone Fischer-Hübner, John Soren Pettersson, Mike Bergmann, Marit Hansen, Siani Pearson, and Marco Casassa Mont</i>	
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
	<i>Tobias Schemer and Lothar Fritsch</i>	
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	A 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
	<i>Stefanie Potzsch, Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, and Sandra Steinbrecher</i>	
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
	<i>Pete Bramhall</i>	
24	Collaborative E-Learning	657
	<i>Katja Liesebach, Elke Franz, Anne-Katrin Stange, Andreas Juschka, Katrin Borcea-Pfitzmann, Alexander Bottcher, and Hagen Wahrig</i>	
24.1	The Collaborative eLearning System BluES'n.	657
24A.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	ChernofT 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
	<i>Jan Zibuschka, Kai Rannenber, and Tobias Kolsch</i>	
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
	<i>Alberto Sanna, Riccardo Serafin, and Nicola Maganetti</i>	
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 Kolsch, Jan Zibuschka, and Kai Rannenber

- 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 Schema769

30.2 Data Handling Language: XML Schema771

Author Index.775