Contents

1 Introduction 1
Kai Rannenberg, Welderufael Tesfay, and Ahmad Sabouri
1.1 Identity Management and its Privacy Issues 1
1.2 Privacy-ABCs for Privacy Enhanced Identity Management 3
1.3 The ABC4Trust Project Goals 4
1.4 Overview of the Pilots 6
1.4.1 Online Course Evaluation 6
1.4.2 School Community Interaction Platform 7
References 9

2 An Architecture for Privacy-ABCs 11
Patrik Bichsel, Jan Camenisch, Maria Dubovitskaya, Robert R. Enderlein, Stephan Krenn, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, Franz-Stefan Preiss, Kai Rannenberg, and Ahmad Sabouri
2.1 Concepts and Features of Privacy-ABCs 12
2.1.1 User Attributes 12
2.1.2 Existing Solutions 14
2.1.3 Basic Concepts of Privacy-ABCs 14
2.1.4 Security and Privacy Features 24
2.2 Architecture Highlights 28
2.3 Architectural Design 29
2.3.1 Overview of the Components 30
2.4 Deployment of the Architecture 33
2.4.1 Setup and Storage 33
2.4.2 Presentation of a Token 36
2.4.3 Issuance of a Credential 38
2.4.4 Inspection 41
2.4.5 Revocation 41

2.5 Language Framework 42
2.5.1 Example Scenario 43
2.5.2 Credential Specification 43
2.5.3 Issuer, Revocation, and System Parameters 44
2.5.4 Presentation Policy with Basic Features 45
2.5.5 Presentation and Issuance Token 48
2.5.6 Presentation Policy with Extended Features 49
2.5.7 Interaction with the User Interface 51
2.6 Applicability to Existing Identity Infrastructures 54
2.6.1 WS-* 54
2.6.2 SAML 56
2.6.3 OpenID 58
2.6.4 OAuth 59
2.6.5 X.509 PKI 62
2.6.6 Integration Summary 65
2.7 Trust Relationships in the Ecosystem of Privacy-ABCs 66
2.7.1 The Meaning of Trust 66
2.7.2 Related Work 67
2.7.3 Trust Relationships 67
2.8 Policy-based View of the Architecture 74
References 75

3 Cryptographic Protocols Underlying Privacy-ABCs 79
Patrik Bichsel, Jan Camenisch, Maria Dubovitskaya, Robert R. Enderlein, Stephan Krenn, Anja Lehmann, Gregory Neven, and Franz-Stefan Preiss
3.1 Overview of Cryptographic Architecture 80
3.1.1 Key Generation Orchestration 81
3.1.2 Presentation Orchestration 82
3.1.3 Verification Orchestration 83
3.1.4 Issuance Orchestration 84
3.1.5 Building Blocks 88
3.1.6 Proof Engine 90
3.2 Cryptographic Primitives 93
3.2.1 Algebraic Background 93
3.2.2 Zero-Knowledge Proofs of Knowledge 95
3.2.3 Commitment Schemes 97
3.2.4 Blind Signature Schemes 99
3.2.5 Verifiable Encryption 103
3.2.6 Scope-Exclusive Pseudonyms 104
3.2.7 Revocation 105
References 107

4 Comparison of Mechanisms . . . 109
Michael Østergaard Pedersen, Gert Læssøe Mikkelsen, Fatbardh Veseli, Ahmad Sabouri, and Tsvetoslava Vateva-Gurova
4.1 Theoretical Comparison – Security Properties and Claims . . . 110
4.1.1 Computational Assumptions . . . 111
4.1.2 Security Aspects of Privacy-ABC Schemes . . . 112
4.1.3 Key Sizes in Practice . . . 114
4.2 Practical Comparison . . . 116
4.2.1 Comparison Criteria for Privacy-ABC Technologies . . . 117
4.2.2 Functionality Comparison . . . 124
4.2.3 Efficiency Comparison . . . 128
4.2.4 Security Assurance Comparison . . . 136
References . . . 139

5 Legal Data Protection Considerations . . . 143
Marit Hansen, Felix Bieker, Daniel Deibler, Hannah Obersteller, Eva Schlehahn, and Harald Zwingelberg
5.1 Legal Requirements . . . 143
5.1.1 Concepts of Anonymity and Pseudonymity . . . 144
5.1.2 Applicable Law . . . 145
5.1.3 General Principles and Protection Goals . . . 145
5.1.4 Legal Roles . . . 148
5.1.5 Legal Grounds . . . 149
5.1.6 Data Security Measures . . . 151
5.2 Applying Legal Requirements to Privacy-ABCs . . . 152
5.2.1 Transparency and Intervenability for Privacy-ABCs . . . 152
5.2.2 Contractual Fixation of Processing on Behalf of the Controller . . . 154
5.2.3 Modelling the Inspection Process . . . 155
5.2.4 Considerations Concerning the Revocation Process . . . 158
References . . . 160

6 School Community Interaction Platform: the Söderhamn Pilot of ABC4Trust . . . 163
Ahmad Sabouri, Souheil Bcheri, Jimm Lerch, Eva Schlehahn, and Welderufael Tesfay
6.1 Application Description . . . 164
6.1.1 Pilot Key Scenarios . . . 164
6.1.2 Requirements . . . 167
6.1.3 The Key Design Elements . . . 168
6.1.4 Security and Privacy Highlights . . . 172
6.2 Deployment and Operation of the Pilot . . . 173
6.2.1 The Deployment Architecture . . . 173
6.2.2 Initialization and the Roll-out Process . . . 177
6.2.3 Specification of the Key Use Cases . . . 178
6.3 Evaluation of the School Pilot . . . 182

6.3.1 Evaluation of the Deployment 182
6.3.2 Evaluation of User Experience........................ 186
6.3.3 Conclusion 193
References 194

7 Course Evaluation in Higher Education: the Patras Pilot of ABC4Trust.. 197
Yannis Stamatiou, Zinaida Benenson, Anna Girard, Ioannis Krontiris, Vasiliki Liagkou, Apostolos Pyrgelis, and Welderufael Tesfay
7.1 Application Description 198
7.1.1 The Basic Requirements and Functionalities of the Pilot . 200
7.1.2 Advanced Features and Functionalities................ 202
7.2 Deployment and Operation of the Pilot 204
7.2.1 The Deployment Architecture 205
7.2.2 Policy Specifications for the Main Use Cases 211
7.3 Evaluation of Usability and User Acceptance of Privacy-ABCs ... 215
7.3.1 Research Questions: Usability and User Acceptance 216
7.3.2 Conceptual Development of a User Acceptance Model .. 217
7.3.3 Additional Factors of User Acceptance 221
7.3.4 Research Methodology 223
7.3.5 Results of User Feedback and Usability Evaluation 227
7.3.6 Results on User Acceptance Factors 229
7.3.7 Insights into the Understanding of Privacy-ABCs 232
7.3.8 Discussion of the Evaluation Results 234
7.3.9 Limitations and Future Work 235
7.4 Conclusion.. 235
References 236

8 Experiences and Feedback from the Pilots...................... 241
Norbert Götze, Daniel Deibler, and Robert Seidl
8.1 The Project Setup 242
8.1.1 Development and Operational Work-Split 242
8.1.2 Processing Contracts between Developers and Operators. 242
8.1.3 Pilot Applications 243
8.2 Lessons Learned from the Pilots 245
8.2.1 Usability 245
8.2.2 Strategy for Adopting Privacy-ABC Technologies 247
8.2.3 Language Support 248
8.2.4 Debugging 248
8.2.5 Bootstrapping the System........................... 249
8.2.6 The Smart Cards 250
8.2.7 Inspector Application Enhancements 251
8.2.8 Some Pitfalls 251
8.2.9 Data Transfer 253
References 254

9 Technical Implementation and Feasibility 255
Gert Læssøe Mikkelsen, Kasper Damgård, Hans Guldager, Jonas Lindstrøm Jensen, Jesus Garcia Luna, Janus Dam Nielsen, Pascal Paillier, Giancarlo Pellegrino, Michael Bladt Stausholm, Neeraj Suri, and Heng Zhang
9.1 The Reference Implementation 256
9.1.1 Obtaining and Compiling the Source Code 257
9.1.2 Deployment of the ABCE as Web Services 261
9.1.3 Integrating the ABCE in Custom Solutions 266
9.1.4 Generating Parameters 268
9.1.5 Example Applications 269
9.1.6 The Hotel Booking Demo Scenario 269
9.1.7 Access Control Based on Birthdate 278
9.1.8 Handling Revocation 280
9.1.9 Setting Up Your Own Test Privacy-ABC System 281
9.1.10 Implementation Considerations 281
9.1.11 Obtaining the ABC4Trust Demo Applications 282
9.2 ABC4Trust in Smart Cards 282
9.2.1 Privacy-ABCs on Smart Cards: Prior Art 282
9.2.2 Introducing ABC4Trust Lite 283
9.2.3 Functional Model for Privacy-ABC Systems 286
9.2.4 Instantiating U-Prove, Idemix and other Privacy-ABC Systems 295
9.2.5 The “Counter” Mechanism 295
9.2.6 Summary of the APDU Command Set 298
9.2.7 Potential Extensions 299
9.3 ABC4Trust on Smartphones 299
9.3.1 ABCE on Android 300
9.3.2 Privacy ABCs in JavaScript 302
9.3.3 Smart Card Emulation 305
9.4 Perturbation Analysis 305
9.4.1 Overall Approach 306
9.4.2 Overview of the PA Methodology 307
9.4.3 Detailed Methodology 311
9.4.4 Detailed Overview of the Results 313
References 315

10 Privacy-ABC Usage Scenarios 319
Joerg Abendroth, Marit Hansen, Ioannis Krontiris, Ahmad Sabouri, Eva Schlehahn, Robert Seidl, and Harald Zwingelberg
10.1 Review of the Main Actors from a Business Perspective 320
10.1.1 User 321
10.1.2 Verifier 322
10.1.3 Issuer (with or without IdM) 323
10.2 Some Typical Privacy-ABC Scenarios 326

10.2.1 Scenario: eIDs . . . 326
10.2.2 Scenario: Anonymous Participation in Decisions and Polls . . . 330
10.2.3 Use of Cloud Service within Enterprises . . . 333
10.2.4 Scenario: Bank as Identity Service Provider . . . 337
10.2.5 Scenario: Do not Track Relying Parties . . . 339
References . . . 342

11 Establishment and Prospects of Privacy-ABCs . . . 345
Marit Hansen, Hannah Obersteller, Kai Rannenberg, and Fatbardh Veseli
11.1 eIDAS Regulation and ABC4Trust . . . 345
11.1.1 Suggestion "Emphasise the Concept of Authentication instead of Identification" . . . 346
11.1.2 Suggestion "Remove Barriers for Privacy-preserving eID Solutions" . . . 348
11.1.3 Suggestion "Clarify Applicability of Data Protection Requirements also for eID Services" . . . 348
11.1.4 Privacy-ABCs in the eIDAS Landscape . . . 349
11.2 How Stakeholders Can Support Privacy-ABCs . . . 350
11.2.1 "State of the Art" and "Best Practice" . . . 350
11.2.2 Support of Stakeholders . . . 352
11.3 Standardization and Certification . . . 354
11.3.1 Framework Standardizations . . . 354
11.3.2 Certification of Presentation Policies . . . 356
References . . . 358

12 Further Challenges . . . 361
Kai Rannenberg, Jan Camenisch, Ahmad Sabouri, and Welderufael Tesfay
12.1 Enabling Users to Manage Their Identities and the Identity Management Process . . . 362
12.1.1 Devices Suitable for Managing Identities . . . 362
12.1.2 Interfaces for Identity Management . . . 363
12.1.3 Minimizing the Installation Effort . . . 364
12.1.4 Additional Services that Help the Users to Manage Their Data and Protect Their Privacy . . . 364
12.2 Usage of Privacy-ABCs by Relying Parties and Service Providers . 365
12.2.1 Boundaries between Different Domains . . . 365
12.2.2 Interoperability and Compatibility with Existing Technologies . . . 366
12.2.3 Enabling Prototypes and Trials . . . 366
12.2.4 Standardization . . . 367

A ABC4Trust Workpackages and Deliverables 369
A.1 Workpackages 369
A.2 Deliverables 370

B ABC4Trust Consortium 373

Contributors 381

Springer

http://www.springer.com/978-3-319-14438-2

Attribute-based Credentials for Trust
Identity in the Information Society
Rannenberg, K.; Camenisch, J.; Sabouri, A. (Eds.)
2015, XV, 391 p. 122 illus., Hardcover
ISBN: 978-3-319-14438-2