Simone Fischer-Hübner
Steven Furnell
Costas Lambrinoudakis (Eds.)

LNCS 4083

Trust, Privacy, and Security in Digital Business

Third International Conference, TrustBus 2006
Kraków, Poland, September 2006
Proceedings

Springer

Simone Fischer-Hübner Steven Furnell
Costas Lambrinoudakis (Eds.)

Trust, Privacy, and Security in Digital Business

Third International Conference, TrustBus 2006
Kraków, Poland, September 2006
Proceedings

Springer

Volume Editors

Simone Fischer-Hübner
Karlstad University
Department of Computer Science
Universitetsgatan 2, 651 88 Karlstad, Sweden
E-mail: simone.fischer-huebner@kau.se

Steven Furnell
University of Plymouth
School of Computing, Communications and Electronics
Network Research Group, Plymouth, PL4 8AA, UK
E-mail: sfurnell@plymouth.ac.uk

Costas Lambrinoudakis
University of the Aegean
Department of Information and Communication Systems Engineering
Karlovassi, 83200 Samos, Greece
E-mail: clam@aegean.gr

Library of Congress Control Number: 2006931261

CR Subject Classification (1998): K.4.4, K.4, K.6, E.3, C.2, D.4.6, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-37750-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-37750-4 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11824633 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4083

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

Lecture Notes in Computer Science

For information about Vols. 1–4044

please contact your bookseller or Springer

Vol. 4180: M. Kohlhase, OMDoc – An Open Markup Format for Mathematical Documents [version 1.2]. XIX, 428 pages. 2006. (Sublibrary LNAI).

Vol. 4163: H. Bersini, J. Carneiro (Eds.), Artificial Immune Systems. XII, 460 pages. 2006.

Vol. 4162: R. Královič, P. Urzyczyn (Eds.), Mathematical Foundations of Computer Science 2006. XV, 814 pages. 2006.

Vol. 4159: J. Ma, H. Jin, L.T. Yang, J.J.-P. Tsai (Eds.), Ubiquitous Intelligence and Computing. XXII, 1190 pages. 2006.

Vol. 4155: O. Stock, M. Schaerf (Eds.), Reasoning, Action and Interaction in AI Theories and Systems. XVIII, 343 pages. 2006. (Sublibrary LNAI).

Vol. 4153: N. Zheng, X. Jiang, X. Lan (Eds.), Advances in Machine Vision, Image Processing, and Pattern Analysis. XIII, 506 pages. 2006.

Vol. 4151: A. Iglesias, N. Takayama (Eds.), Mathematical Software - ICMS 2006. XVII, 452 pages. 2006.

Vol. 4146: J.C. Rajapakse, L. Wong, R. Acharya (Eds.), Pattern Recognition in Bioinformatics. XIV, 186 pages. 2006. (Sublibrary LNBI).

Vol. 4144: T. Ball, R.B. Jones (Eds.), Computer Aided Verification. XV, 564 pages. 2006.

Vol. 4139: T. Salakoski, F. Ginter, S. Pyysalo, T. Pahikkala, Advances in Natural Language Processing. XVI, 771 pages. 2006. (Sublibrary LNAI).

Vol. 4138: X. Cheng, W. Li, T. Znati (Eds.), Wireless Algorithms, Systems, and Applications. XVI, 709 pages. 2006.

Vol. 4137: C. Baier, H. Hermanns (Eds.), CONCUR 2006 – Concurrency Theory. XIII, 525 pages. 2006.

Vol. 4134: K. Yi (Ed.), Static Analysis. XIII, 443 pages. 2006.

Vol. 4133: J. Gratch, M. Young, R. Aylett, D. Ballin, P. Olivier (Eds.), Intelligent Virtual Agents. XIV, 472 pages. 2006. (Sublibrary LNAI).

Vol. 4130: U. Furbach, N. Shankar (Eds.), Automated Reasoning. XV, 680 pages. 2006. (Sublibrary LNAI).

Vol. 4129: D. McGookin, S. Brewster (Eds.), Haptic and Audio Interaction Design. XII, 167 pages. 2006.

Vol. 4128: W.E. Nagel, W.V. Walter, W. Lehner (Eds.), Euro-Par 2006 Parallel Processing. XXXIII, 1221 pages. 2006.

Vol. 4127: E. Damiani, P. Liu (Eds.), Data and Applications Security XX. X, 319 pages. 2006.

Vol. 4124: H. de Meer, J.P. G. Sterbenz (Eds.), Self-Organising Systems. XIV, 261 pages. 2006.

Vol. 4121: A. Biere, C.P. Gomes (Eds.), Theory and Applications of Satisfiability Testing - SAT 2006. XII, 438 pages. 2006.

Vol. 4119: C. Dony, J.L. Knudsen, A. Romanovsky, A. Tripathi (Eds.), Advanced Topics in Exception Handling Components. X, 302 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - Crypto 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4115: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Computational Intelligence and Bioinformatics, Part III. XXI, 803 pages. 2006. (Sublibrary LNBI).

Vol. 4114: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Computational Intelligence, Part II. XXVII, 1337 pages. 2006. (Sublibrary LNAI).

Vol. 4113: D.-S. Huang, K. Li, G.W. Irwin (Eds.), Intelligent Computing, Part I. XXVII, 1331 pages. 2006.

Vol. 4112: D.Z. Chen, D. T. Lee (Eds.), Computing and Combinatorics. XIV, 528 pages. 2006.

Vol. 4111: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. VIII, 447 pages. 2006.

Vol. 4109: D.-Y. Yeung, J.T. Kwok, A. Fred, F. Roli, D. de Ridder (Eds.), Structural, Syntactic, and Statistical Pattern Recognition. XXI, 939 pages. 2006.

Vol. 4108: J.M. Borwein, W.M. Farmer (Eds.), Mathematical Knowledge Management. VIII, 295 pages. 2006. (Sublibrary LNAI).

Vol. 4106: T.R. Roth-Berghofer, M.H. Göker, H. A. Güvenir (Eds.), Advances in Case-Based Reasoning. XIV, 566 pages. 2006. (Sublibrary LNAI).

Vol. 4104: T. Kunz, S.S. Ravi (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XII, 474 pages. 2006.

Vol. 4099: Q. Yang, G. Webb (Eds.), PRICAI 2006: Trends in Artificial Intelligence. XXVIII, 1263 pages. 2006. (Sublibrary LNAI).

Vol. 4098: F. Pfenning (Ed.), Term Rewriting and Applications. XIII, 415 pages. 2006.

Vol. 4097: X. Zhou, O. Sokolsky, L. Yan, E.-S. Jung, Z. Shao, Y. Mu, D.C. Lee, D. Kim, Y.-S. Jeong, C.-Z. Xu (Eds.), Emerging Directions in Embedded and Ubiquitous Computing. XXVII, 1034 pages. 2006.

Vol. 4096: E. Sha, S.-K. Han, C.-Z. Xu, M.H. Kim, L.T. Yang, B. Xiao (Eds.), Embedded and Ubiquitous Computing. XXIV, 1170 pages. 2006.

Vol. 4094: O. H. Ibarra, H.-C. Yen (Eds.), Implementation and Application of Automata. XIII, 291 pages. 2006.

Vol. 4093: X. Li, O.R. Zaïane, Z. Li (Eds.), Advanced Data Mining and Applications. XXI, 1110 pages. 2006. (Sublibrary LNAI).

Vol. 4092: J. Lang, F. Lin, J. Wang (Eds.), Knowledge Science, Engineering and Management. XV, 664 pages. 2006. (Sublibrary LNAI).

Vol. 4091: G.-Z. Yang, T. Jiang, D. Shen, L. Gu, J. Yang (Eds.), Medical Imaging and Augmented Reality. XIII, 399 pages. 2006.

Vol. 4090: S. Spaccapietra, K. Aberer, P. Cudré-Mauroux (Eds.), Journal on Data Semantics VI. XI, 211 pages. 2006.

Vol. 4089: W. Löwe, M. Südholt (Eds.), Software Composition. X, 339 pages. 2006.

Vol. 4088: Z.-Z. Shi, R. Sadananda (Eds.), Agent Computing and Multi-Agent Systems. XVII, 827 pages. 2006. (Sublibrary LNAI).

Vol. 4085: J. Misra, T. Nipkow, E. Sekerinski (Eds.), FM 2006: Formal Methods. XV, 620 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4082: K. Bauknecht, B. Pröll, H. Werthner (Eds.), E-Commerce and Web Technologies. XIII, 243 pages. 2006.

Vol. 4081: A. M. Tjoa, J. Trujillo (Eds.), Data Warehousing and Knowledge Discovery. XVII, 578 pages. 2006.

Vol. 4080: S. Bressan, J. Küng, R. Wagner (Eds.), Database and Expert Systems Applications. XXI, 959 pages. 2006.

Vol. 4079: S. Etalle, M. Truszczyński (Eds.), Logic Programming. XIV, 474 pages. 2006.

Vol. 4077: M.-S. Kim, K. Shimada (Eds.), Geometric Modeling and Processing - GMP 2006. XVI, 696 pages. 2006.

Vol. 4076: F. Hess, S. Pauli, M. Pohst (Eds.), Algorithmic Number Theory. X, 599 pages. 2006.

Vol. 4075: U. Leser, F. Naumann, B. Eckman (Eds.), Data Integration in the Life Sciences. XI, 298 pages. 2006. (Sublibrary LNBI).

Vol. 4074: M. Burmester, A. Yasinsac (Eds.), Secure Mobile Ad-hoc Networks and Sensors. X, 193 pages. 2006.

Vol. 4073: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), Smart Graphics. XI, 263 pages. 2006.

Vol. 4072: M. Harders, G. Székely (Eds.), Biomedical Simulation. XI, 216 pages. 2006.

Vol. 4071: H. Sundaram, M. Naphade, J.R. Smith, Y. Rui (Eds.), Image and Video Retrieval. XII, 547 pages. 2006.

Vol. 4070: C. Priami, X. Hu, Y. Pan, T.Y. Lin (Eds.), Transactions on Computational Systems Biology V. IX, 129 pages. 2006. (Sublibrary LNBI).

Vol. 4069: F.J. Perales, R.B. Fisher (Eds.), Articulated Motion and Deformable Objects. XV, 526 pages. 2006.

Vol. 4068: H. Schärfe, P. Hitzler, P. Øhrstrøm (Eds.), Conceptual Structures: Inspiration and Application. XI, 455 pages. 2006. (Sublibrary LNAI).

Vol. 4067: D. Thomas (Ed.), ECOOP 2006 – Object-Oriented Programming. XIV, 527 pages. 2006.

Vol. 4066: A. Rensink, J. Warmer (Eds.), Model Driven Architecture – Foundations and Applications. XII, 392 pages. 2006.

Vol. 4065: P. Perner (Ed.), Advances in Data Mining. XI, 592 pages. 2006. (Sublibrary LNAI).

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 394 pages. 2006.

Vol. 4062: G. Wang, J.F. Peters, A. Skowron, Y. Yao (Eds.), Rough Sets and Knowledge Technology. XX, 810 pages. 2006. (Sublibrary LNAI).

Vol. 4061: K. Miesenberger, J. Klaus, W. Zagler, A.I. Karshmer (Eds.), Computers Helping People with Special Needs. XXIX, 1356 pages. 2006.

Vol. 4060: K. Futatsugi, J.-P. Jouannaud, J. Meseguer (Eds.), Algebra, Meaning, and Computation. XXXVIII, 643 pages. 2006.

Vol. 4059: L. Arge, R. Freivalds (Eds.), Algorithm Theory – SWAT 2006. XII, 436 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4057: J.P.W. Pluim, B. Likar, F.A. Gerritsen (Eds.), Biomedical Image Registration. XII, 324 pages. 2006.

Vol. 4056: P. Flocchini, L. Gąsieniec (Eds.), Structural Information and Communication Complexity. X, 357 pages. 2006.

Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), Data Engineering Issues in E-Commerce and Services. IX, 290 pages. 2006.

Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.

Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.

Vol. 4052: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part II. XXIV, 603 pages. 2006.

Vol. 4051: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part I. XXIII, 729 pages. 2006.

Vol. 4049: S. Parsons, N. Maudet, P. Moraitis, I. Rahwan (Eds.), Argumentation in Multi-Agent Systems. XIV, 313 pages. 2006. (Sublibrary LNAI).

Vol. 4048: L. Goble, J.-J.C.. Meyer (Eds.), Deontic Logic and Artificial Normative Systems. X, 273 pages. 2006. (Sublibrary LNAI).

Vol. 4047: M. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4046: S.M. Astley, M. Brady, C. Rose, R. Zwiggelaar (Eds.), Digital Mammography. XVI, 654 pages. 2006.

Vol. 4045: D. Barker-Plummer, R. Cox, N. Swoboda (Eds.), Diagrammatic Representation and Inference. XII, 301 pages. 2006. (Sublibrary LNAI).

¥385.00元

Preface

This book presents the proceedings of the Third International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2006), held in Kraków, Poland, September 5-7, 2006. The conference continues from previous events held in Zaragoza (2004) and Copenhagen (2005), and maintains the aim of bringing together academic researchers and industry developers to discuss the state of the art in technology for establishing trust, privacy and security in digital business. We thank the attendees for coming to Kraków to participate and debate the new emerging advances in this area.

The conference programme included two keynote presentations, one panel session and eight technical papers sessions. The keynote speeches were delivered by Jeremy Ward from Symantec EMEA on the topic of "Building the Information Assurance Community of Purpose", and by Günter Karjoth from IBM Research - Zurich, with a talk entitled "Privacy Practices and Economics — From Privacy Policies to Privacy SLAs."

The subject of the panel discussion was "Is Security Without Trust Feasible?" chaired by Leszek T. Lilien from Western Michigan University, USA. The reviewed paper sessions covered a broad range of topics, from access control models to security and risk management, and from privacy and identity management to security protocols. The conference attracted 70 submissions, each of which was assigned to four referees for review. The Programme Committee ultimately accepted 24 papers for inclusion, which were revised based upon comments from their reviews.

We would like to express our thanks to the various people who assisted us in organizing the event and formulating the programme. We are very grateful to the Programme Committee members, and external reviewers, for their timely and rigorous reviews of the papers. Thanks are also due to the DEXA Organizing Committee for supporting our event, and in particular to Mrs. Gabriela Wagner for her help with the administrative aspects. We would also like to thank Sokratis Katsikas, Javier López and Günther Pernul for their past efforts in establishing the conference series, and their valuable advice and assistance in enabling us to take it forward.

Finally we would like to thank all of the authors who submitted papers for the event, and contributed to an interesting set of conference proceedings.

September 2006
Kraków, Poland

Simone Fischer-Hübner, Karlstad University, Sweden
Steven Furnell, University of Plymouth, UK
Costas Lambrinoudakis, University of the Aegean, Greece

Programme Committee

General Chair

Simone Fischer-Hübner	Karlstad University, Sweden

Programme Committee Co-chairs

Steven Furnell	University of Plymouth, UK
Costas Lambrinoudakis	University of the Aegean, Greece

International Programme Committee Members

Alessandro Acquisti	Carnegie Mellon University, USA
Marco Casassa Mont	HP Labs, Bristol, UK
David Chadwick	University of Kent, UK
Nathan Clarke	University of Plymouth, UK
Frederic Cuppens	ENST Bretagne, France
Ernesto Damiani	University of Milan, Italy
Ed Dawson	Queensland University of Technology, Australia
Claudia Eckert	Darmstadt Technical University, Germany
Hannes Federrath	University of Regensburg, Germany
Eduardo B. Fernandez	Florida Atlantic University, USA
Elena Ferrari	University of Insubria at Como, Italy
Juan M. González-Nieto	Queensland University of Technology, Australia
Rüdiger Grimm	University of Koblenz , Germany
Dimitrios Gritzalis	Athens University of Economics and Business, Greece
Stefanos Gritzalis	University of the Aegean, Greece
Ehud Gudes	Ben-Gurion University, Israel
Sigrid Gürgens	Fraunhofer Institute for Secure Information Technology, Germany
Marit Hansen	Independent Center for Privacy Protection, Germany
Audun Josang	School of Software Engineering & Data Communications, QUT, Australia
Tom Karygiannis	NIST, USA
Sokratis Katsikas	University of the Aegean, Greece
Dogan Kesdogan	RWTH Aachen University, Germany
Hiroaki Kikuchi	Tokai University, Japan

Spyros Kokolakis	University of the Aegean, Greece
Klaus Kursawe	Philips Research, Eindhoven, The Netherlands
Leszek Lilien	Western Michigan University, USA
Antonio Lioy	Politecnico di Torino, Italy
Javier López	University of Malaga, Spain
Peter Lory	University of Regensburg, Germany
Olivier Markowitch	Université Libre de Bruxelles, Belgium
Fabio Martinelli	National Research Council – CNR Pisa, Italy
Fabio Massacci	University of Trento, Italy
Jose A. Montenegro	University of Malaga, Spain
Eiji Okamoto	University of Tsukuba, Japan
Martin S. Olivier	University of Pretoria, South Africa
Rolf Oppliger	eSecurity Technologies, Switzerland
Maria Papadaki	University of Plymouth, UK
Ahmed Patel	Centre for Applied Research in Information Systems, Kingston University, UK
Günther Pernul	University of Regensburg, Germany
Andreas Pfitzmann	Dresden University of Technology, Germany
Hartmut Pohl	University of Applied Sciences, FH Bonn-Rhein-Sieg, Germany
Karl Posch	University of Technology, Graz, Austria
Torsten Priebe	Capgemini, Austria
Gerald Quirchmayr	University of Vienna, Austria
Kai Rannenberg	Goethe University of Frankfurt, Germany
Christoph Ruland	University of Siegen, Germany
Pierangela Samarati	University of Milan, Italy
Matthias Schunter	IBM Zurich Research Lab., Switzerland
Mikko T. Siponen	University of Oulu, Finland
Adrian Spalka	University of Bonn, Germany
Leon Strous	De Nederlandsche Bank, The Netherlands
Stephanie Teufel	University of Fribourg, Switzerland
Jianying Zhou	I2R, Singapore

External Reviewers

Isaac Agudo	University of Malaga, Spain
Manos Antonakakis	NIST, USA
Aimilios Apostolopoulos	NIST, USA
Giampaolo Bella	University of Catania, Italy
Rainer Böhme	Dresden University of Technology, Germany

Katrin Borcea-Pfitzmann	Dresden University of Technology, Germany
Colin Boyd	Queensland University of Technology, Australia
Andrew Clark	Queensland University of Technology, Australia
Sebastian Clauß	Dresden University of Technology, Germany
Nora Cuppens-Boulahia	ENST Bretagne, France
Wiebke Dresp	University of Regensburg, Germany
Ludwig Fuchs	University of Regensburg, Germany
Dimitris Geneiatakis	University of the Aegean, Greece
Juhani Heikka	University of Oulu, Finland
Christos Kalloniatis	University of the Aegean, Greece
Costas Karafasoulis	University of the Aegean, Greece
George Karopoulos	University of the Aegean, Greece
Maria Karyda	University of the Aegean, Greece
Tobias Koelsch	RWTH Aachen University, Germany
Stefan Köpsell	Dresden University of Technology, Germany
Hristo Koshutanski	Create-Net, Italy
Ponnurangam Kumaraguru	Carnegie Mellon University, USA
Dimitris Lekkas	University of the Aegean, Greece
Mink Martin	RWTH Aachen University, Germany
Patrick Sinclair Merten	University of Fribourg, Switzerland
Nicola Mezzetti	Università di Bologna, Italy
Björn Muschall	University of Regensburg, Germany
Andriy Panchenko	RWTH Aachen University, Germany
Lexi Pimenidis	RWTH Aachen University, Germany
Carsten Rudolph	Fraunhofer Institute for Secure Information Technology, Germany
Rolf Schillinger	University of Regensburg, Germany
Christian Schläger	University of Regensburg, Germany
Sandra Steinbrecher	Dresden University of Technology, Germany
Martin Steinert	University of Fribourg, Switzerland
Daniela Wanner	University of Fribourg, Switzerland
Andreas Westfeld	Dresden University of Technology, Germany
Nicola Zannone	University of Trento, Italy

Table of Contents

Session 1: Privacy and Identity Management

Session 2: Security and Risk Management

Session 3: Security Requirements and Development

Session 4: Privacy Enhancing Technologies and Privacy Management

Session 5: Access Control Models

Session 6: Trust and Reputation

Session 7: Security Protocols

Session 8: Security and Privacy in Mobile Environments

Towards Scalable Management of Privacy Obligations in Enterprises

Marco Casassa Mont

Hewlett-Packard Labs, Trusted Systems Lab
Bristol, UK
marco.casassa-mont@hp.com

Abstract. Privacy management is important for enterprises that collect, store, access and disclose personal data. Among other things, the management of privacy includes dealing with privacy obligations that dictate duties and expectations an enterprise has to comply with, in terms of data retention, deletion, notice requirements, etc. This is still a green area open to research and innovation: it is about enabling privacy-aware information lifecycle management. This paper provides an overview of the work we have done in this space: definition of an obligation management model and a related framework; implementation of a prototype of an obligation management system integrated both in the context of the PRIME project and with an HP identity management solution. This paper then focuses on an important open issue: how to make our approach scalable, in case large amounts of personal data have to be managed. Thanks to our integration work and the feedback we received, we learnt more about how users and enterprises are likely to deal with privacy obligations. We describe these findings and how to leverage them. Specifically, in the final part of this paper we introduce and discuss the concepts of parametric obligation and "hybrid" obligation management and how this can improve the scalability and flexibility of our system. Our work is in progress. Further research and development is going to be done in the context of the PRIME project and an HP Labs project.

1 Introduction

Enterprises that store, manage and process personal data must comply with privacy laws and satisfy people's expectations on how their personal data should be used. Privacy laws [1,2,3] dictate policies on how personal data should be collected, accessed and disclosed according to stated purposes, by keeping into account the consent given by data subjects (e.g. customers, employees, business partners) and by satisfying related *privacy obligations* including data retention, data deletion, notice requirements, etc.

The management and enforcement of privacy policies in enterprises is still a green field: key requirements include automation, cost reduction, simplification, compliance checking and integration with existing enterprise identity management solutions. In particular the management of *privacy obligations* is open to research and innovation. Privacy obligations [4] dictate duties and expectations on how personal data should be

S. Fischer-Hübner et al. (Eds.): TrustBus 2006, LNCS 4083, pp. 1 – 10, 2006.

managed. They require enterprises to put in place *privacy-aware information lifecycle management* processes.

During the last two years we have been active in the *privacy obligation management* [5] space by: (1) researching and defining an explicit model for privacy obligations; (2) formalising the representation of obligations; (3) introducing an obligation management framework and a related *obligation management system* to deal with the explicit scheduling, enforcement and monitoring of privacy obligations.

This paper provides an overview of the current status of this work. Our current obligation management system allows end-user to customise - in a fine-grained way - their personal preferences: related privacy obligations (based on the set of obligations supported by an enterprise) are automatically generated and associated to users' data. However, this causes scalability issues when large sets of personal data have to be managed, because our system generates a large set of associated privacy obligations: their current management is expensive and inefficient. Addressing this aspect is very important for enterprises that potentially have to deal with millions of data records related to customers, employees or business partners.

The integration phase of our work in PRIME [6] and with an HP identity management solution [8, 12] and the feedback we received from third parties (customers, HP businesses, etc.) has helped us to better understand how users are actually likely to define their privacy preferences and which realistic support enterprises can provide in terms of handling privacy obligations. We describe these findings and highlight how they can actually be leveraged to address the scalability issues. The final part of this paper describes our related ideas, based on the concept of *parametric obligations* and *a hybrid obligation management model*. This work is in progress and will be carried on in the context of PRIME and an HP Labs project.

2 Management of Privacy Obligations in Enterprises

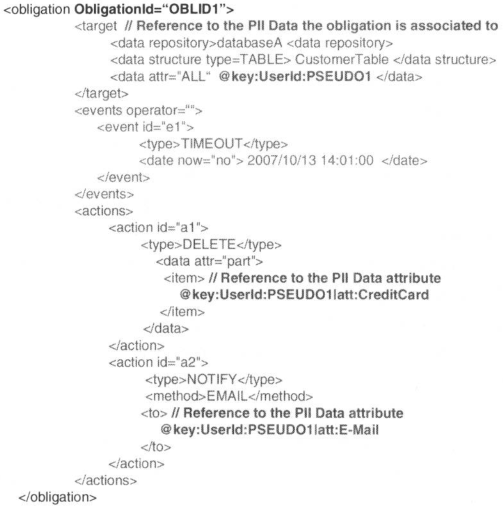
This section provides a quick overview of our R&D work to manage privacy obligations in enterprises. Details can be found in [4,5,9].

Privacy obligations [4,5,9] are policies that dictate expectations and duties to enterprises on how to handle personal data and how to deal with its lifecycle management in a privacy-aware way. They include: dealing with data deletion and retention, dealing with data transformation (e.g. encryption), sending notifications, executing workflows involving human and system interactions, logging information, etc.

Related work includes EPAL [10] that defines a privacy language, inclusive of a placeholder for obligations, in the context of an Enterprise Privacy Authorisation architecture [11]. This is important work but it does not define obligation policies in detail and subordinate their enforcement to access control. Similar observations apply for XACML [8] and other work in the obligation management space.

In our vision the management and enforcement of privacy obligations must not be subordinated to the management and enforcement of access control policies [4]. For example, deletion of personal data at a precise point in time has to happen independently from the fact that this data has ever been accessed. This fundamental concept is at the very base of our work and differentiates it from related work. A more detailed comparison of our work against related work is provided in [4,5,9].

Based on this concept, we introduced an *obligation management model* [4,5,9], where privacy obligations are "first class" entities, i.e. they are explicit entities that are modeled, managed and enforced. In this model, a privacy obligation is an "object" [9] that includes: *Obligation Identifier*; T*argeted Personal Data* (e.g. data affected by the obligation); *Triggering Events* (e.g. time-based events); *Actions* (e.g. data deletion, sending notifications) – see Figure 1.



```
<obligation ObligationId="OBLID1">
        <target  // Reference to the PII Data the obligation is associated to
              <data repository>databaseA <data repository>
              <data structure type=TABLE> CustomerTable </data structure>
              <data attr="ALL"  @key:UserId:PSEUDO1 </data>
        </target>
        <events operator="">
           <event id="e1">
                 <type>TIMEOUT</type>
                 <date now="no"> 2007/10/13 14:01:00  </date>
           </event>
        </events>
        <actions>
              <action id="a1">
                    <type>DELETE</type>
                       <data attr="part">
                        <item> // Reference to the PII Data attribute
                           @key:UserId:PSEUDO1|att:CreditCard
                        </item>
                     </data>
              </action>
              <action id="a2">
                     <type>NOTIFY</type>
                     <method>EMAIL</method>
                    <to> // Reference to the PII Data attribute
                       @key:UserId:PSEUDO1|att:E-Mail
                    </to>
              </action>
        </actions>
</obligation>
```

Fig. 1. Simple Example of Privacy Obligation

Figure 1 shows a very simple example of a privacy obligation (expressed in XML), associated to the personal data of a user (in the example having the *PSEUDO1* unique identifier) and stored in an enterprise RDBMS database. This obligation dictates the deletion of a personal attribute (credit card detail) at a predefined point in time, along with the need to notify the user via e-mail when this happens.

In general, our privacy obligations can target personal data stored in various types of data repositories, including databases, LDAP directories, meta/virtual directories, file systems, etc. This further differentiates our work and approach from related work, that is mainly focused on the management of data in RDBMS databases, e.g. [13].

We designed an *obligation management framework* [4,5,9] and an associated *obligation management system* [4,5,9] to represent these privacy obligations, schedule and enforce them and monitor for their the fulfillment. In our system, *data subjects* (i.e. users) can explicitly define privacy preferences (e.g. on data deletion, notifications, etc.) on their personal data at their disclosure time (e.g. during a self-registration process) or at any subsequent time. These preferences are automatically turned into privacy obligations, based on the types of obligations supported by an enterprise. *Enterprise privacy administrators* can further associate other privacy obligations to personal data, for example dictated by laws or internal guidelines.

As a proof-of-concept, a working prototype has been fully implemented and integrated in the context of the EU PRIME project [6]. To demonstrate the feasibility and applicability of this work within enterprises, we also integrated it with HP OpenView Select Identity (an HP state-of-the-art identity management solution [7]) to manage privacy preferences and related privacy obligations during user provisioning and account management processes.

3 Scalability Issues

Our obligation management system provides flexible, fine-grained mechanisms to end-users (and enterprise privacy administrators) to express their privacy preferences (e.g. deletion preferences, notification preferences, etc.) on their personal data: based on the types of obligations supported by an enterprise, our system automatically turns these preferences into privacy obligations (by means of translation rules) and manages them. Users have the capability to customize aspects of these obligations (e.g. actual combinations of events and actions) as long as they are supported by the enterprise. The side-effect of this flexibility (at least in the current implementation) is that for each piece of personal data disclosed by a user, one or more privacy obligations can be generated, each of them with its own specific properties and requirements. For example, each user of an e-commerce site could potentially specify different privacy preferences (e.g. deletion date, notification preferences, encryption of data, data minimisation, etc.) and privacy constraints (among the ones supported by the enterprise) on their personal data. Figure 2 shows this approach (architectural details are omitted for simplicity).

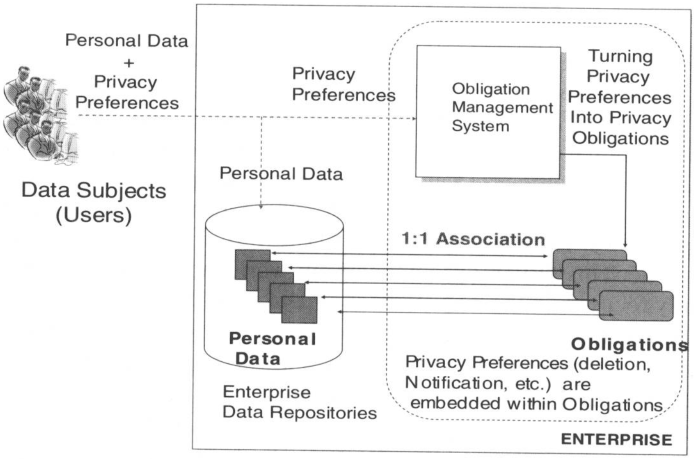


Fig. 2. Current Model: Direct Association of Privacy Obligations to Personal Data

In case large amounts of users are managed by the enterprise, large amounts of privacy obligations are created and subsequently they must be explicitly scheduled, enforced and monitored by our obligation management system. In general, the