Springer Theses
Recognizing Outstanding Ph.D. Research

Ghazi Ben Ayed

Architecting User-Centric Privacy-as-a-Set-of-Services

Digital Identity-Related Privacy Framework

Springer

Springer Theses

Recognizing Outstanding Ph.D. Research

For further volumes:
http://www.springer.com/series/8790

Aims and Scope

The series "Springer Theses" brings together a selection of the very best Ph.D. theses from around the world and across the physical sciences. Nominated and endorsed by two recognized specialists, each published volume has been selected for its scientific excellence and the high impact of its contents for the pertinent field of research. For greater accessibility to non-specialists, the published versions include an extended introduction, as well as a foreword by the student's supervisor explaining the special relevance of the work for the field. As a whole, the series will provide a valuable resource both for newcomers to the research fields described, and for other scientists seeking detailed background information on special questions. Finally, it provides an accredited documentation of the valuable contributions made by today's younger generation of scientists.

Theses are accepted into the series by invited nomination only and must fulfill all of the following criteria

- They must be written in good English.
- The topic should fall within the confines of Chemistry, Physics, Earth Sciences, Engineering and related interdisciplinary fields such as Materials, Nanoscience, Chemical Engineering, Complex Systems and Biophysics.
- The work reported in the thesis must represent a significant scientific advance.
- If the thesis includes previously published material, permission to reproduce this must be gained from the respective copyright holder.
- They must have been examined and passed during the 12 months prior to nomination.
- Each thesis should include a foreword by the supervisor outlining the significance of its content.
- The theses should have a clearly defined structure including an introduction accessible to scientists not expert in that particular field.

Ghazi Ben Ayed

Architecting User-Centric Privacy-as-a-Set-of-Services

Digital Identity-Related Privacy Framework

Doctoral Thesis accepted by
University of Lausanne, Switzerland

Springer

Author
Dr. Ghazi Ben Ayed
Faculty of Business and Economics (HEC)
Department of Information Systems
University of Lausanne
Lausanne
Switzerland

Supervisor
Prof. Solange Ghernaouti
Faculty of Business and Economics (HEC)
Department of Information Systems
University of Lausanne
Lausanne
Switzerland

ISSN 2190-5053 ISSN 2190-5061 (electronic)
ISBN 978-3-319-08230-1 ISBN 978-3-319-08231-8 (eBook)
DOI 10.1007/978-3-319-08231-8
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014941917

Printed on acid-free paper

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

Parts of this thesis have been published in the following articles:

- Ben Ayed, G., Ghernaouti-Hélie, S., **Service-Oriented Digital Identity-related Privacy Interoperability: Implementation Framework of Privacy-as-a-Set-of-Services (PaaSS)** 2012 4th International IFIP Working Conference on Enterprise Interoperability (IWEI), pp. 193–200 http://link.springer.com/chapter/10.1007%2F978-3-642-33068-1_18
- Ben Ayed, G., Ghernaouti-Hélie, S., **Architecting Interoperable Privacy within User-Centric Federated Digital Identity Systems: Overview of a Service-Oriented Implementation Framework** 2012 4th International Conference on Networked Digital Technologies (NDT), pp. 165–177 http://link.springer.com/chapter/10.1007%2F978-3-642-30567-2_14
- Ben Ayed, G., Ghernaouti-Hélie, S., **Disassembling Digital Identity-Related Privacy into a Set of Services: SoaML-based Services Design** 2012 3rd International Conference on Exploring Services Sciences (IESS), pp. 44–57 http://link.springer.com/chapter/10.1007%2F978-3-642-28227-0_4
- Ben Ayed, G., Ghernaouti-Hélie, S., **Privacy Requirements Specification for Digital Identity Management Systems Implementation: Towards a digital society of privacy** 2011 6th IEEE International Conference for Internet Technology and Secured Transactions (ICITST), pp. 602–607
- Ben Ayed, G., Ghernaouti-Hélie, S., **Digital Identity Management within Networked Information Systems: From Vertical Silos View into Horizontal User-Supremacy Processes Management** 2011 14th IEEE International Conference on Network-Based Information Systems (NBiS), pp. 98–103
- Ben Ayed, G., Ghernaouti-Hélie, S., **Digital Identity Attributes Cohesion to Access E-services: Major Issues and Challenges in Digital Society** (2011) Journal of E-Technology, Volume 2, Number 3, pp. 89–97
- Ben Ayed, G., Ghernaouti-Hélie, S., **XRD Digital Identity Metadata-Based Approach to Foster Collaborations across Networked Computing Ecosystems** 2011 3rd International Conference on Networked Digital Technologies (NDT), pp. 105–119 http://link.springer.com/chapter/10.1007%2F978-3-642-22185-9_10
- Ben Ayed, G., **Digital Identity Metadata Scheme: A technical approach to reduce digital identity risks** 2011 International Workshop on Information Security and Risk management of the 25th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 607–612
- Ben Ayed, G., **Consolidating Fragmented Identity: Attributes Aggregation to Secure Information Systems** 2008 IADIS International Conference on Information Systems, elected through blind review process as **Best Position Paper**

To the Lord Almighty

Supervisor's Foreword

As a professor in the Faculty of Business and Economics at the University of Lausanne, Director of the Swiss Cybersecurity Advisory and Research Group, I had the privilege and pleasure of supervising the doctoral research of Ghazi Ben Ayed, a body of research that led to a Ph.D. thesis entitled: "Architecting User-Centric Privacy-as-a-Set-of-Services: Digital Identity Related Privacy Framework."

In this work, Dr. Ben Ayed has developed a global and systematic approach to the problems of the management of digital identities and of maintaining confidence in the systems used for such identity management. He proposed elements of solutions for allowing digital identities and the parameters associated with these identities, essentially private data, to be managed by their owners and only made visible and available according to criteria defined by those owners. In doing so he contributed to the protection of personal data while considering the relevant technical and legal constraints.

Of particular note were his interdisciplinary approach, validated through the creation and verification of models for confidence and assurance, and his innovative approach towards proposing a technical solution to guarantee the right for data to be forgotten.

Along with the other members of the examining panel, I was struck by the quality of the research and of the practical solutions that were presented: these demonstrated a clear mastery of the conceptual principles of the field as well as of technical and technological matters. Specifically, Dr. Ben Ayed's research required finding answers to the central question of how to design and implement interoperable privacy systems based on the use of digital identities. The response consisted of developing a framework based on the needs for privacy created by the use of digital identities, designing Privacy as a Set-of-Services (PaaSS), and demonstrating how this could be implemented within the framework of Service-Oriented Architecture (SOA).

As a visionary in this field, Ghazi has been able to anticipate and pre-empt the description of the needs for the protection of personal data and of privacy in the age of the information society. With political, economic, legal, and technical stakes at play, the control of digital data has become a widespread desire. Real

wars are breaking out around this new search for power and profits. Espionage, surveillance and the manipulation of information are current affairs and nobody can now be unfamiliar with the dangers linked to weaknesses in data protection. Through his work Ghazi ben Ayed demonstrates the existence of new possibilities for the owners of digital data to protect those data. He provides them with the means of re-establishing control over their own information assets and shows that it is not necessary to remain powerless in the face of the abusive and inappropriate use of our private data.

Lausanne, March 2014 Prof. Solange Ghernaouti

Preface

This work has been elected the best thesis in information systems in the information systems department, Faculty of Business and Economics, University of Lausanne, Switzerland (2012). It has also been nominated for European Research Consortium for Informatics and Mathematics (ERCIM) Best Ph.D. Thesis Award on Security and Trust Management (2013) and for Faculty's Outstanding Dissertation Award, Faculty of Business and Economics, University of Lausanne, Switzerland (2012). Additionally, the first published article of this work has been awarded "Best Position Paper" in one of the international conferences in information systems (2008).

We present the approach and results of work that has been conducted at the Department of Information Systems (ISI), University of Lausanne, Switzerland. We consider this work as a crutial step towards the realization of our **service-oriented cyber-security vision**: Could cyber-security be delivered a set of autonomous hosted services available per request on per-usage basis? We leave an increasingly digital footprint in cyberspace and this situation puts our digital identity at high risks. Privacy is a right and fundamental social value that could secure digital identities. Thus, the main question of this research is how to turn digital identity-related privacy in a shape of set of services that are loosely coupled, publicly hosted and available to on-demand calls. It is recognized that technical initiatives are not enough to guarantee resolution for the concerns surrounding a multifaceted and complex issue of identity and privacy. For this reason they should be apprehended within a global perspective through an integrated and a multidisciplinary approach, which dictates that privacy law, policies, regulations and technologies are to be crafted together from the beginning of the project as a set of requirements. They are drawn from global, domestic, and business-specific privacy laws and policies related to digital identity. We suggest a layered implementation DigIdeRP framework in accordance to model-driven architecture approach that would help cyber-security team to implement security requirements in the form of a set of services that could accommodate Service-Oriented Architecture (SOA): Privacy-as-a-Set-of-Services (PaaSS) system. The framework will serve as a basis for vital understanding between business management and technical managers on digital identity-related privacy initiatives. The layered framework presents

five practical layers as an ordered sequence as a basis of security project roadmap, however, in practice, there is an iterative process to assure that each layer supports effectively and enforces requirements of the adjacent ones. Each layer is composed of a set of blocks, which determine a roadmap that security team could follow to successfully implement PaaSS. Several blocks' descriptions are based on OMG SoaML modeling language and BPMN processes description. We identified, designed, and implemented services that form PaaSS and described their consumption. PaaSS Java (JEE project), WSDL, and XSD codes are given and explained.

April 2014 Dr. Ghazi Ben Ayed

Acknowledgments

I would like to express my gratitude to every person who contributed and helped both directly and indirectly to make this doctoral project in the best conditions. In particular:

I would like to express my sincere gratitude to my Ph.D. supervisor Prof. Solange Ghernaouti-Hélie for the valuable guidance and advices. Her generosity and willingness to motivation contributed tremendously to the achievement.

I have been fortunate in having unwavering support of my mother Zahra and my father Abdelwaheb. My vocabulary fails me in thanking them for their guidance, understanding, and patience from my young age. I do warrant a special recognition.

I am grateful to the love of my life Nourchène, son Mohamed Reyam, and daughter Kenza for all the sacrifices. Heartfelt and endless thanks go to all my family members, in particular my beautiful sisters, brothers-in-law, and parents-in-law for their encouragement and support to pursue my interests. Words will never be strong enough to express my recognition and my deepest gratitude.

I want to do justice to my own teachers in helping me to broaden my view and knowledge. A special thank you to the teaching body of école primmaire El-Menzah5 and lycée secondaire El-Menzah6, Tunis, Tunisia; Institut Supérieur de Gestion-University of Tunis, Tunisia; McGill University, HEC Montréal, University of Montreal, Canada; and University of Lausanne, Switzerland.

Last, but not least, my gratitude is extended to all my research colleagues who continue to share their wealth of knowledge in order to make the digital world a safer environment and to turn it from an “un-forgetting” into a “forgiving” place.

Contents

Acronyms

BPMN	Business Process Model and Notation
CCNx	Content-Centric Networks
DigIdM	Digital Identity Management
DigIdDoc	Digital Identity Document
DigIdMeta	Digital Identity MetaEngine
DigIdeRP	Digital Identity-Related Privacy
FIM	Federated Identity Management
IdP	Identity Provider
IS	Information Systems
PaaSS	Privacy-as-a-Set-of-Services
PET	Privacy-Enhanced Technologies
SOA	Service-Oriented Architectures
SoaML	Service-oriented architecture Modeling Language
SP	Service Provider

Chapter 1
Introduction and Motivations

There is a powerful tension in our relationship to technology.
We are excited by egalitarianism and anonymity,
but we constantly fight for our identity.
David Owens (Professor at Vanderbilt University)

1.1 Context and Research Motivations

The advent of Internet-compliant technologies and open standards are easing the extension of information systems by lowering the barriers to connecting disparate business applications both within and across corporate boundaries. Increasingly, information technology architects are asked to define end-to-end business processes that span borders to enable inter-enterprise collaborations and mass integration with partners. Therefore, the current fortress landscape becomes a puzzle of partnering enterprises that should be working hand-in-hand toward building a common defense program in order to fortify the security of critical resources available within and across information systems [1]. Identity management systems span technological, political and social boundaries, and have become a strategic requirement for today's enterprise. Organizations could achieve both tactical benefits for the present and strategic benefits for the future. They can immediately benefit from regulations' compliance, such as privacy, security will be improved, fraud will be minimized and operating costs will be reduced [2]. Particularly, identity federation scheme, such as the Identrus consortium,[1] supports re-use of credentials and infrastructure to minimize cost and it supports the separation of authentication and attributes stores, allowing privacy and data control issues to be managed [3]. Thus, efficient management of digital identities is a critical need of the agile and profitable enterprise [4].

[1] http://www.identrust.com

G. Ben Ayed, *Architecting User-Centric Privacy-as-a-Set-of-Services*, Springer Theses,
DOI: 10.1007/978-3-319-08231-8_1, © Springer International Publishing Switzerland 2014

Identity and privacy are complex concepts and should be studied from different perspectives, thus, a multidisciplinary approach becomes a necessity. The complexity of managing identity and privacy comes from multiple reasons such as the nature of identity and privacy that have multiple facets: technological, social, legal, and cultural; and the fragility of digital identity bounded with immaturity of privacy in the digital life [5, 6]. Moreover, it is questioned whether information privacy and security are positively correlated in some situations and negatively correlated in others? And how stable or dynamic is the relationship between them is different technological settings and organizational environments? In addition and depending on the situation, users face identity retention and disclosure tradeoff. Sometimes, they are obliged to disclose digital identities but sometime users refrain from sharing digital identity to prevent possible exposure and privacy breaches; and in another side they disclose digital identity attributes and other information to make online transactions, seek convenience, and have fun. In the offline world, anonymous transactions can be conducted successfully, but in the service-oriented online world trust should be established between parties [7–9]. There are times when individuals need a secure and an accurate representation of themselves and other times when people may want to have the ability and freedom to project a quite different persona in online world to that in the offline world [10]. Moreover, these conflicting needs and requirements are compounded by a technological capability that is moving far too fast for society and companies to adapt to [11]. Additionally, the diversity of regulations and privacy policies rise transborders issues because they are set with different intents, purpose, and outcomes increases complexities [12]. Thus, a technical approach is not sufficient enough to tackle privacy issues and Privacy-enhanced Technologies (PET) is an example of technical initiative failure [10]. They have proved useful only in very narrow domains and did not respond adequately to the online world needs [13, 14]. A multidisciplinary and integrated approach dictates that law, policies, regulations and technologies are to be crafted together.

Internet is being criminalized. The fraudulent use of individual identity has increased at an alarming rate, thus privacy and identity management can play a key role to secure participation in digital society. Digital identity is bringing a whole new dimension to our existing identities. We leave an increasingly digital footprint in cyberspace such as digital records of our prenatal scans available on Flickr, personal profile within a social networks, death information in FamilySearch[2] historical records, data collected by diverse agencies on our behalf, blogs' contributions, emails, performed searches with various engines. Trails are memorized by the network, while, in most cases, we still don't have the capabilities to delete them if we wish. Major online service providers memorize, access, and exploit 'Web of trails' for their own commercial benefits, and as a result, we are losing control over our personal data and leaving our identity at a high risk. One hundred million worldwide Facebook users are threatened by identity theft as

[2] http://fsbeta.familysearch.org/

a repercussion of Facebook hack case [15], in which personal details have been collated and published on file-sharing service. The dramatic increase in identity theft and other types of digital identity is unlikely to end soon. Security, identity theft, incorrect computer records, credit rating destruction, privacy, online purchasing and banking, loss of identity, misuse of personal information, phishing, identity cards, behavioral monitoring and tracking, etc. The list of concerns is long and people still feel concerned and worried about the digital world, security and loss of control. Criminal forces have organized themselves internationally to trick users into releasing valuable information through phishing schemes, to inadvertently install spyware in users' computers and harvests information through pharming attacks, or to stealing a vast amount of identities by targeting corporate, government and educational databases. Criminal networks are working toward acquiring and reselling identities and the international character of these networks makes them increasingly difficult to penetrate and dismantle. Privacy is a critical right and protection to enforce, if we wish to provide to individuals with the means to secure and control their digital identities, while enabling organizations to exploit fairly this invaluable source of information. When privacy is compromised, security of the individual, the organization or the country could be threatened [7, 10, 11, 16–21].

Identity and privacy should be interoperable and distributed through the adoption of service-orientation and implementation based on open standards. Identity functionality is increasingly delivered as sets of services, rather than monolithic applications. It is hard to create an identity layer for the internet mainly due to the little agreement on what it should be done and how it should be run. The lack of agreement arises because digital identity is contextual in nature. Thus the emergence of a single simplistic universal digital identity solution is not realistic [17]. Privacy is to be engineered to integrate identity from the start, rather than attaching it to identity after the fact. It is confirmed that building secure systems requires privacy principles/policies to be taken into consideration from the early stage [2, 22]. Design must start from maximum of privacy is one of the design principles of European PRIME Project [23]. Organizations are realizing that they need better security, particularly identity and privacy management through a better interoperability both within and between countries. Interoperability is not just technical interoperability but the alignment of policy, services and processes with business requirements [24]. W3C Platform for Privacy Preferences (P3P) Project is a step towards interoperability by making privacy policies of web sites transparent for automated agents but the use of SSL to protect connections to public sites and deployment of Kerberos within enterprises lacked global vision and they've been implemented only for specific domains. Service-Oriented Architectures (SOA) is widely used in distributed and dynamic systems and driving a loosely coupled approach to application interoperability and integration [25]. We borrow OMG SoaML SOA definition: "SOA is a way of describing and understanding organizations, communities and systems to maximize agility, scale and interoperability". SOA defines how people, organizations and systems provide and

use services to achieve results [26]. In system that is implemented following the SOA approach, functionalities are delivered and consumed as services [27]. SOA aims to simplify development and delivery of new business functionalities, enabling reusability and interoperability. Thus, services would be built according to a prescribed set of standards, protocols, and interfaces, which make them interoperable and reusable [28]. Thus, an identity layer in which identity and privacy management services are loosely coupled, publicly hosted and available to on-demand calls could be more realistic and an acceptable situation.

Digital identity management projects requires a set of guidelines and advices [18], Oracle suggested best practices and SOA governance framework [29] to help make SOA implementation projects. Thus, there is a need to build a framework to better manage implementation risks and encourage stakeholders work together, collaboratively throughout the process as a team. The framework allows people, processes, and technology to be collaboratively integrated [30].

1.2 Problem Statement and Research Outcomes

In this thesis, we aim to respond to the following main questions: how identity architects and designers could design interoperable digital identity-related privacy system? Other questions are also important to respond in order to be able to answer the main research question: how to capture business interoperability described in the form of digital identity-related privacy (DigIdeRP) requirements? How to disassemble business interoperability into set of services (technical interoperability): Privacy-as-a-Set-of-Services (PaaSS) system? The research is information system design-type in the field of security and its outcome is to suggest a layered framework to help security implementation team to design, architect, and implement PaaSS system. The framework relays on the idea that privacy requirements should be taken into consideration from the beginning of system development project and privacy regulations/policies could be incorporated into technology. Service-oriented architecture modeling language (SoaML) diagrams are used to convert requirements into set of services.

Digital identity attributes are supposed to be shared after setting up a contract between parties. In Fig. 1.1, the subject asks for a service from the service provider (SP), which gives back a digital identity-related privacy contract form. The subject chooses to accept terms of privacy contract then the SP asks the required digital identity attributes. The subject replies by specifying Identity Provider(s) IdP(s) that SP should reach. Involved IdP(s) contact the subject in order to receive digital identity attributes release confirmation. The subject confirms, IdP(s) release attributes and SP gives the service to the subject. Various SPs and IdPs are distributed within a circle-of-trust (discontinued line eclipse) and collaborate with the subject to deliver the service. Parties involved in circle-of-trust should have been already agreed to comply with terms of privacy contract. Such distributed environment imposes the need of interoperability to execute and apply terms and

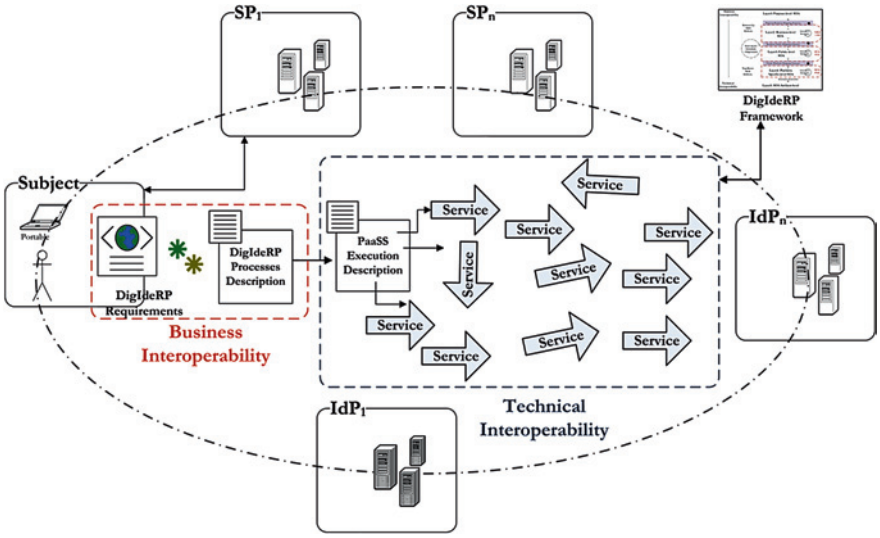

Fig. 1.1 Technical and business interoperability

conditions of privacy contract between parties. With the emergence of service-oriented architecture and open standards as means of interoperability, we suggest a five-layer DigIdeRP implementation framework to disassemble terms and conditions of privacy contract into a set of collaborated services: Privacy-as-a-Set-of-Services (PaaSS) system.

Following steps of the framework, we began with identification of business interoperability, through the definition of DigIdeRP requirements that are drawn from global, domestic and business-specific privacy policies. DigIdeRP requirements enumerate a set of objectives capable of being widely enough accepted to serve as backplane for distributed systems. Because these requirements are drawn from major privacy policies, they reflect a remarkable convergence of interests and organizational will to implement them. Each requirement ends up giving rise to an architectural principle guiding the construction of PaaSS. The framework is not only a technical-view framework, rather, it is multidisciplinary and multiple views framework that gather different roles and responsibilities in implementation security team. Top level security management is responsible for specification of the purpose-level SOA (layer1); security/privacy business analysts are responsible of business-level SOA (layer2); security/privacy architects are responsible of fabric-level SOA (layer3); and security/privacy systems developers are responsible of platform-specific-level SOA (layers4) and SOA-Artifacts-level (layer5). Mapping gateways ensure the transition between two layers, thus layers' owners have to collaborate and communicate to successfully conduct the mapping. Mapping gateways help to avoid siloed implementation and assure a shared effort. Flow chart diagrams and documents could facilitate the communication between owners and contribute to the success of the mapping.

DigIdeRP Framework helps to align DigIdeRP initiatives with organization's business goals and security strategy. Such initiative requires an engagement from top level security management throughout the project. The framework's components are distributed over five layers and three mapping gateways to define the roadmap that security implementation team should follow to successfully conduct the project. The framework allows not only service identification, design, and implementation but also service executions to support DigIdeRP requirements translated into BPMN business processes. The framework is enough flexible to allow multi-perspectives services implementation. It allows implementing services based on range of perspectives: network operator centric perspective, application service provider centric perspective, or user-centric perspective. In each perspective, we should describe the requirements in the form of conversation and information exchange between SP, IdP, and Subject. Even if the DigIdM technical model is not identity federation, centralization could be a good candidate, see Chap. 3. Because it is built in accordance to model-driven approach, the framework should accelerate the implementation because it could be supported by a range of design and implementation tools in order to have automatic code generation.

1.3 Thesis Outline

After introducing the thesis by setting the scene, describing research motivations and justifications, and specifying the research question, we provide high-level dissertation structure and a brief summary of the major contributions in each chapter as follows. We discuss in Chap. 2 multiple facets and fundamentals of digital identity and describe major issues and complexities surrounding digital identity. However, in Chap. 3, we provide taxonomy of digital identity management (DigIdM) definitions based on three types of definition-focus: technical, management, and user-supremacy. We explain that DigIdM should have a horizontal process view and service orientation. We provide a description and comparison between DigIdM technical models and we give supremacy to digital identity federation and particularly to its derivate user-centricity. We propose an innovative approach based on Metadata usage to make less visible persistent digital identity documents, thus, users would be given more control over digital identity information. We implement this approach on Content-Centric Networks (CCNx). In Chap. 4, we discuss the basics of privacy and issues surrounding digital identity-related privacy. We study and group privacy policies into three policy classes: global, domestic and business-specific privacy policies. We draw DigIdeRP requirements from these privacy policies related to digital identity. Ten DigIdeRP requirements are identified: purpose specification of attributes collection, consent for attributes usage and release, limited usage of attributes, limited retention of attributes, accuracy of stored attributes, openness, authentication and enrollment needs, choice and terms of the contract, secondary use, and compliance. These requirements will be considered as a starting point to implement

target's Privacy-as-a-Set-of-Services system. We provide, in Chap. 3, an overview of the Service-oriented Architecture (SOA) foundations and we explain DigIdeRP Framework in accordance of model driven engineering approach to implement PaaSS system, a technical interoperability. Such implementation requires business interoperability: DigIdeRP requirements. The requirements are described on business processes basis with Business Process Model and Notation (BPMN). Six DigIdeRP processes are identified and explained. We choose OMG Service Oriented Architecture Modeling Language (SoaML) to identify and describe the pool of autonomous, granular and loosely coupled services. The BPMN processes description combined with SoaML services' description allows defining service consumption roadmap. We present in Chap. 6 SoaML design toolkit and SOA artifacts of the user-centric digital identity federation participants (SP, IdP, and Subject). Few corresponding pieces of codes are given with explanations. Finally, a brief summary conclusions and main research contribution are included in Chap. 7. We identify research limits and several areas of future research work and improvements.

References

1. G. Ben Ayed, Consolidating fragmented identity: attributes aggregation to secure information systems. IADIS Int. J. Comput. Sci. Info. Syst. **4**, 1–12 (2009)
2. P. Mackinnonm, in *Large-Scale Identity Management in Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, ed. by D.G.W. Birch (Gower Publishing Limited, Farnham, 2007), pp. 105–112
3. J. Skipper, in *Authentication in Business in Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, ed. by D.G.W. Birch (Gower Publishing Limited, Farnham, 2007), pp. 95–104
4. A. Scorer, in *Identity Directories and Databases, in Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, ed. by D.G.W. Birch (Gower Publishing Limited, Farnham, 2007)
5. H. Noonan, B. Curtis, "*Identity*", in *Stanford Encyclopedia of Philosophy* (2009), Available: http://plato.stanford.edu/entries/identity/
6. E. Dallaway, Loss of privacy: internet security's high price. Infosecurity Magazine **4**(7), 10 (Elsevier, 2007)
7. P.J. Windley, *Digital Identity: Unmasking identity management architecture* (IMA) (O'Reilly Media, California, 2005)
8. M. Benantar, *Access Control Systems: Security, Identity Management and Trust Models* (Springer, Berlin, 2006)
9. S. Clauβ, M. Köhntopp, Identity management and its support of multilateral security. Comput. Netw. Int. J. Comp. Telecommun. Netw. **37**(2), 205–219 (2001)
10. International Telecommunication Union, Digital life. ITU internet report. (2006), Available http://www.itu.int/osg/spu/publications/digitalife/docs/digital-life-web.pdf. Accessed 21 May 2010
11. P. Cochrane, in "*Forward of the Book*," *in Digital Identity Management: Perspectives on the Technological, Business and Social Implications*, ed. by D.G.W. Birch (Gower Publishing Limited, Farnham, 2007)