Service-Oriented Digital Identity-Related Privacy Interoperability: Implementation Framework of Privacy-as-a-Set-of-Services (PaaSS)

Ghazi Ben Ayed, Solange Ghernaouti-Hélie

Service-Oriented Digital Identity-related Privacy Interoperability: Implementation Framework of Privacy-as-a-Set-of-Services (PaaSS)

Ghazi Ben Ayed[1], Solange Ghernaouti-Hélie[1]

[1] Information Systems Institute, Faculty of Business and Economics, University of Lausanne, CH-1015, Lausanne, Switzerland
{Ghazi.Benayed, Sgh}@unil.ch

Abstract. Protecting digital identity is crucial aspect in order to successfully enable collaboration between heterogeneous and distributed information systems. In this context, privacy could play a key role for digital identity protection and security. Thus, an identity layer in which interoperable privacy is delivered in the shape of a set of services, rather than monolithic applications, would be inevitably responding to the need of collaboration. In this article, we suggest a novel layered service-oriented implementation framework that information systems security projects' members could borrow to successfully turn digital identity-related privacy requirements into a set of services. Several blocks are distributed amongst five layers and three mapping gateways determine the roadmap of the implementation effort governance. Seven loosely coupled, publicly hosted and available to on-demand calls services are specified to accommodate service-oriented architectures. OMG SoaML diagrams, BPMN process descriptions and SOA-artifacts specifications are provided and explained.

Keywords: Digital identity, privacy, interoperability, implementation framework, SOA.

1 Introduction

Recent years have seen the trend of business globalization which urgently requires dynamical collaboration among organizations. The business processes and organizations' information systems need to be integrated seamlessly to adapt the continuously changing business conditions and to stay competitive in the global market. Collaborative environments present major challenges to privacy since there is an exchange of digital identities between collaborators [1]. Moreover, privacy is a critical right and a protection to enforce, if we wish to provide to individuals with the means to protect digital identities. When privacy is compromised, security of the individual, the organization or the country could be threatened [2-10]. Thus, there is a need to establish a balance between the benefits of collaborative environments, which

provide knowledge discovery and sharing against the protection of individual and organizational privacy needs [11].

A technical approach is not sufficient enough to tackle privacy issues and Privacy-enhanced Technologies (PET) is an example of technical initiative failure [7]. We promote a multidisciplinary and integrated approach, which dictates that law, policies, regulations and technologies are to be crafted together. Moreover, digital identity management functionalities are increasingly delivered as sets of services, rather than monolithic applications. So, an identity layer in which identity and privacy management are interoperable could respond to the need of distributed environments. Such interoperability could be offered through design of a set of loosely coupled, publicly hosted and available to on-demand calls services and implementations on open standards.

In this article, we aim to respond to the following main questions: how we could implement interoperable digital identity-related privacy (DigIdeRP) system? Narrowly, how to disassemble digital identity-related privacy business interoperability into a technical interoperability in the shape of set of services: 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 service-oriented implementation governance framework that could help information system's security designers, architects, and developers to turn DigIdeRP requirements into a set of services that can domicile a service-oriented architecture (SOA). The framework relays on the idea that privacy is to be engineered to integrate identity from the start, rather than attaching it to identity after the fact. The implementation governance 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. This article is organized as follows. In section 2, we explain the need of interoperable privacy within federated digital identity systems and we describe the target PaaSS system. In section 3, we describe each block of the implementation governance framework that could help information system's security implementation team to successfully conduct DigIdeRP interoperability initiatives in the shape of PaaSS system. We identify seven services through the use of OMG SoaML modeling language from DigIdeRP requirements and we describe services' consumption with BPMN flow-chart based notation. We provide a range of SoaML diagrams to illustrate the design and pre-implementation steps. Finally, we conclude and present future work in section 4.

2 Layered SO-DigIdeRP Implementation Framework

Oracle suggested best practices within SOA governance framework [12] to help guide SOA implementation projects. In general, a framework can help to better manage implementation risks and encourage stakeholders work together, collaboratively throughout the process as a team. In addition, it allows people, processes, and technology to be collaboratively integrated [13]. The framework serves as a basis for vital understanding between business and technical managers on how to collaborate in order to conduct such initiatives. In earlier work [14] , we presented an overview of

the framework but here we suggest various blocks that we dispatch over five layers and three mapping gateways, see figure 1. The blocks in the Service-Oriented Digital Identity-related Privacy (SO-DigIdeRP) framework determines a roadmap that security team could follow to successfully implement interoperability.

2.1 Layer1, Layer2 and Mapping Gateway

In the purpose-level SOA layer, we articulate the need of implementing DigIdeRP initiatives, which are to be approached from a strategic point of view with a high level of clarity on objectives. In the purpose-business mapping gateway, we identify the privacy requirements sources related to digital identity such as policies, fair information practices, laws and procedures. In business-level SOA layer, we specify four blocks: 1) functional requirements' specification. Ten DigIdeRP requirements [15] are already specified and detailed; 2) digital identity management (DigIdM) technical model specification. Technical models are already been covered and compared in [16] in which digital identity federation is elected because it secures distributed systems and allows better privacy protection; 3) specification of DigIdM deployment perspective. ITU report [17] classifies DigIdM systems' works and projects into a landscape of three perspectives: a) network operator centric perspective in which capabilities that maximize and protect network assets are sought; b) application service provider centric perspectives in which capabilities that maximize and protect application assets are sought; and c) user-centric perspective in which capabilities that allow privacy protection and user control over digital identity are sought. Considered as a derivate of digital identity federation, user-centric digital identity federation is a novel and promising approach that provides more control over digital identity [18]. That's why user-centric approach is adopted. DigIdM technical model and DigIdM deployment perspective blocks are grouped into DigIdM architectural model envelope; and 4) the business process portray deals with providing process-based view of DigIdeRP requirements. Six DigIdeRP processes are identified and described in flow-chart Business Process Modeling Notation (BPMN 2.0). The processes are: a) ServiceRequest process; b) ProfileToChallenge process: the subject sends a profile-to-challenge-request to the SP in order to be able to access his profile, check its validity and have the capability to change it. The SP sends the possessed profile that is drawn from digital identity attributes aggregation. The subject may send a change, update or modify profile request to the SP, which confirms the update operation. However, no action will be undertaken if the subject is in agreement with his profile, see figure 2; c) EnrollmentRequest process; d) DigitalIdentityToUpdate process; e) PeriodicDigitalIdentityToUpdate process; and f) EditDigitalIdentity process.

2.2 Layer3 and Service Design Approach

SoaML is an OMG specification, which describes a UML profile and metamodel for designing services within a service-oriented architecture. SoaML is chosen for two major reasons: 1) SoaML is a modeling language that helps to ensure an easy

understanding and validation by the project members since SoaML permits a technology-neutral representation of the services; 2) SoaML supports the activities for modeling service that could be accommodated by service oriented architecture. SoaML permits to identify service candidates and to design services for SOA and not SOA itself [19].

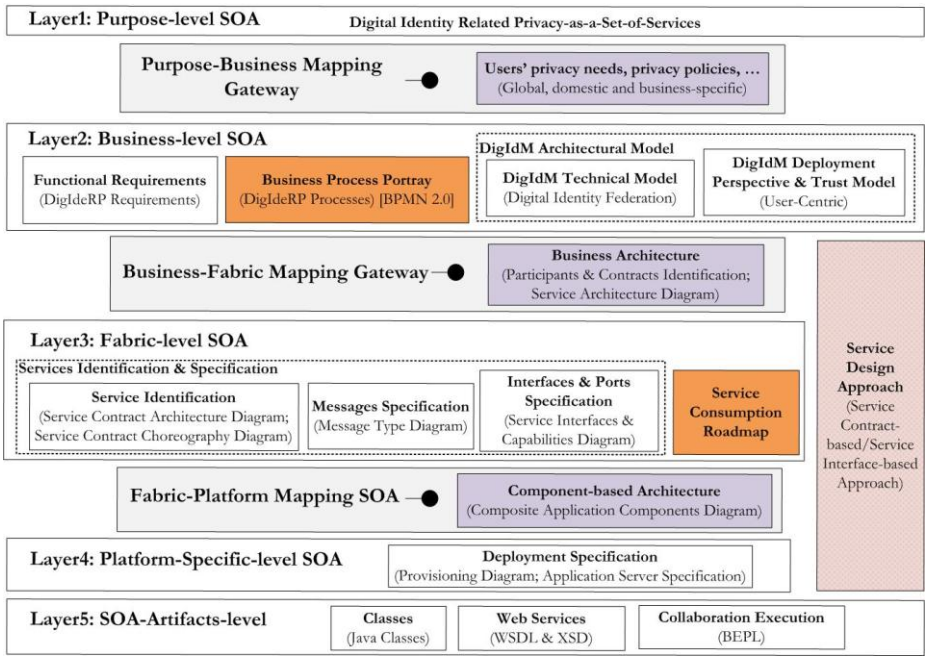

Fig. 1. Layers and blocks of SO-DigIdeRP implementation framework

Service design approach is an inter-layers block. SoaML modeling capabilities support the service "contract-based" and "interface-based" approaches [20]. We had to choose between the two approaches before undertaking activities in the business-fabric mapping gateway, fabric-platform mapping gateway, layer 3, and layer 4.The service-contract approach requires an already established business and collaboration agreement between parties. In the adopted DigIdM identity federation technical model, circle-of-trust sets the agreement between parties of the identity federation, thus, service-contract approach is the best-fit.

In the business-fabric mapping gateway, we set the SoaML service architecture diagram to define participants and service contracts. We define seven service contracts, which would be later on seven services. We identify participants (subject, IdP, SP) that participates in a service contract with either a "sender" or "receiver" role, which may change when participants participate in other service contracts. For instance, in the ProfileToChallenge service contract, the Subject plays the role of a sender and the SP as a receiver and in DigitalIdentityRequest service contract the senders are the Subject and IdP; and the receiver is SP. In the fabric-level SOA, we define seven services without regard for their implementations: 1) ContractAgreement

service; 2) DigitalIdentityRequest service; 3) DigitalIdentityToUpdate service; 4) PeriodicDigitalIdentityToUpdate service; 5) Enrollment service; 6) ProfileToChallenge service; and 7) EditDigitalIdentity service. For each service, we provide details through establishment of SoaML service contract architecture diagram, service contract choreography diagram, and message type diagram. Each service contract diagram shows though a connector that an interaction is established between two roles stereotyped "consumer" and "provider". Methods are available either in consumer service interface or provider service interface. The latter can invoke methods that are available through consumer service interface and vice-versa. The service choreography diagram highlights the negotiation and communication process between service interfaces in term of calls of methods. Moreover, different inputs of the methods are messages that are described in messages diagrams.

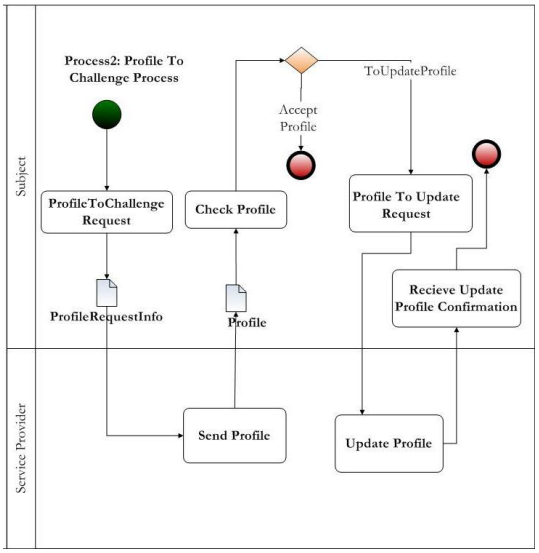

Fig. 2. BPMN Description of ProfileToChallenge Process

In figure 3, the service contract is established between the consumer ProfileToChallengeReceiver and the provider ProfileToChallengeSender. Each role is represented by an interface. The consumer invokes ProfileRequest with profileProperties message type, which encloses subjectRef information. The provider invokes sendProfile method with profile message type. The consumer is able to send a request for a profile change by invoking profileToUpdateRequest method with profile properties message type. The provider receives a profile change acknowledgement as a result of consumer's invocation of updateProfileConfirmation method with UpdatedProfileConfirmation message type.

In the service consumption roadmap, we combine BPMN process description with SoaML service identification and specification in order to define how services are consumed to execute processes. To execute ProfileToChallenge process, the service ProfileToChallenge is consumed four times with different methods and following this order: 1) (Service Name: ProfileToChallenge Service, Requester: Subject, Recipient:

SP, Method: ProfileRequest); 2) (Service Name: ProfileToChallenge Service, Requester: SP, Recipient: Subject, Method: SendProfile); 3) (Service Name: ProfileToChallenge Service, Requester: Subject, Recipient: SP, Method: ProfileToUpdateRequest); and 4) (Service Name: ProfileToChallenge Service, Requester: SP, Recipient: Subject, Method: UpdateProfileConfirmation).

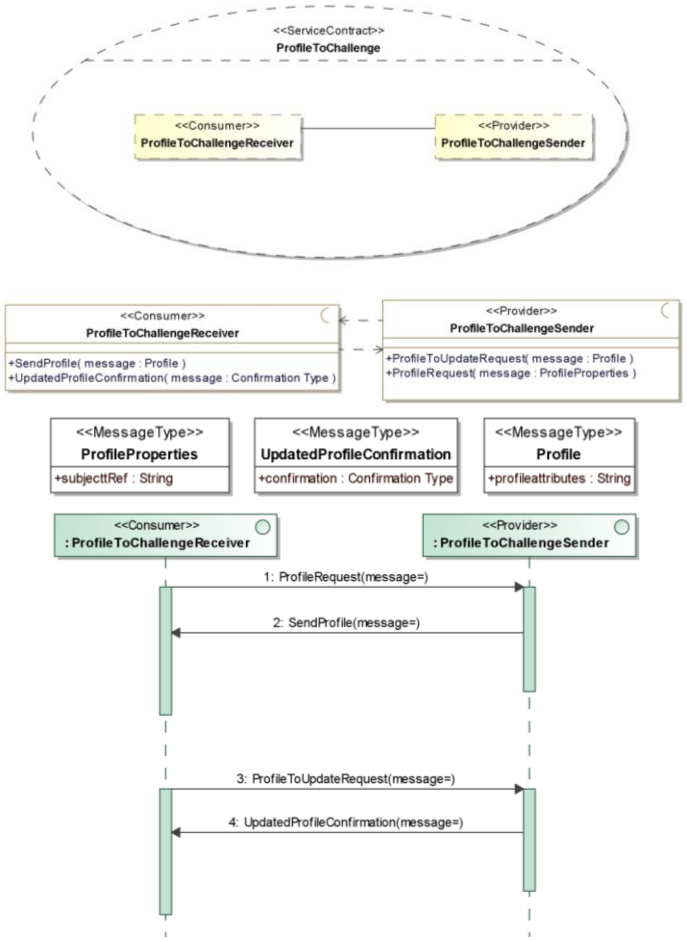

Fig. 3: ProfileToChallenge service contract, message type and choreography diagrams

2.3 Layer 4, Layer5 and Mapping Gateway

In the fabric-platform mapping, we describe, through SoaML composite application component diagram, different components to be implemented. The composite application component diagram is a platform-independent diagram; however, the provision diagram, in layer 4, is a platform-dependent one. We implement in Java Enterprise Edition, the provision diagram. We integrated Eclipse IDE (version 3.4)

with ModelPro SDK (version 1.1) in order to generate the code of SOA-related artifacts, layer5, including Java code for service interfaces and SCA components, and XSD, WSDL, SCA Composite files.

3 Conclusion and Outlooks

SO-DigIdeRP framework blocks descriptions are based on OMG SoaML, which helps to systemically choose and identify services on the basis of service contracts specifications. We intend to explore the existence and applicability of other service modeling languages on SO-DigIdeRP framework and to compare framework outputs. While SoaML service contracts has provided a major contribution to model DigIdeRP requirements, but we find that it also interesting to explore the development of DigIdeRP requirements with RuleML and to evaluate benefits and inconveniences against possibilities that are offered by SoaML. We intend also to implement services from network operator centric perspective and application service provider centric perspective based on the description of each DigIdM deployment perspective requirements. Moreover, we will adopt service interface based approach instead of service contract based approach and we'll explore differences. The major limit of the framework is services longevity issue. When DigIdeRP requirements, DigIdM technical models, deployment or trust models changes, impacts of the changes affect the design and implementation of all services at a risk of existing services reutilization. This is due to the tightly-coupled nature of DigIdeRP requirements. Metamodel for privacy policies within SOA of [21-23] in which researchers have made a decomposition of privacy policies, and it is inspiring us to conduct future research to explore whether the service identification starts from requirements disassembling rather than from service design.

References

[1] Y. Duan and J. Canny, "Protecting User Data in Ubiquitous Computing: Towards Trustworthy Environments," *LNCS Springer,* 2005.

[2] S. Philippsohn, "ID and the Law," in *Digital Identity Management: Perspectives on the Technological, Business and Social Implications* D. G. W. Birch, Ed., ed: Gower Publishing Limited 2007, pp. 193-203.

[3] P. Cochrane, "Forward of the Book," in *Digital Identity Management: Perspectives on the Technological, Business and Social Implications* D. G. W. Birch, Ed., ed: Gower Publishing Limited 2007.

[4] K. Cameron, "The Laws of Identity," ed: Microsoft Corporation, 2005.

[5] M. Hansen*, et al.*, "Privacy and Identity Management," *IEEE Security & Privacy,* 2008.

[6] G. Bell and J. Gemmel. (2007) A Digital Life. *Scientific American Magazine*. 58-65.

[7] International Telecommunication Union. (2006), Digital Life. *ITU Internet Report*

[8] P. J. Windley, *Digital Identity: Unmasking identity management architecture (IMA)*: O'Reilly Media, 2005.
[9] K. Cukier. (2010) A special report on managing information. *The Economist (February 23rd-March 5th)*.
[10] Organizing Committee of Digital Identity & Privacy (Human Capital & Social Innovation Technology Summit). (2007), *Call for Controbution to Managing Digital Identities for Education, Employment and Business Development*.
[11] V. Bellotti, "What You Don't Know Can Hurt You: Privacy in Collaborative Computing," in *British Computer Society Conference on Human-Computer Interaction*, 1996, pp. 241 - 261.
[12] M. Afshar*, et al.* (2007), *SOA Governance: Framework and Best Practices*
[13] D. Kelley. (2009), Practical Approaches for Securing Web Applications across the Software Delivery Lifecycle.
[14] G. Ben Ayed and S. Ghernaouti-Hélie, "Architecting Interoperable Privacy within User-Centric Federated Digital Identity Systems: Overview of a Service-Oriented Implementation Framework," in *the 4th International Conference on Networked Digital Technologies (NDT 2012)*, Canadian University of Dubai, United Arab Emirates, 2012, pp. 165-177.
[15] G. Ben Ayed and S. Ghernaouti-Hélie, "Privacy Requirements Specification for Digital Identity Management Systems Implementation: Towards a digital society of privacy," in *6th International Conference for Internet Technology and Secured Transactions (ICITST-2011)*, Abu Dhabi, UAE, 2011.
[16] G. Ben Ayed, "Consolidating Fragmented Identity: Attributes Aggregation to Secure Information Systems," *IADIS International Journal on Computer Science and Information Systems,* vol. 4, pp. 1-12, 2009.
[17] ITU Focus Group on Identity Management (FG IdM), "Report on Identity Management Use Cases and Gap Analysis," 2007.
[18] A. Jøsang and S. Pope, "User-Centric Identity Management," in *Proceedings of the AusCERT Asia Pacific Information Technology Security Conference*, 2005, pp. 1-6.
[19] OMG. (2009), Service oriented architecture Modeling Language (SoaML) - Specification for the UML Profile and Metamodel for Services (UPMS).
[20] B. Elvesæter*, et al.*, "Specifying Services Using the Service Oriented Architecture Modeling Language (SoaML): A baseline for specification of cloud-based services," in *The 1st International Conference on Cloud Computing and Services Science (CLOSER 2011)*, Noordwijkerhout, The Netherlands, 2011.
[21] D. S. Allison*, et al.*, "Privacy and trust policies within SOA " in *International Conference for Internet Technology and Secured Transactions (ICITST 2009)*, 2009.
[22] D. S. Allison*, et al.*, "Metamodel for privacy policies within SOA," in *The 2009 ICSE Workshop on Software Engineering for Secure Systems (IWSESS '09)* 2009.
[23] D. Garcia*, et al.*, "An Electronic Contract Model for Privacy Protection in Service-Oriented Architecture," in *Fifth International Conference on Digital Information Management (ICDIM 2010)*, Thunder Bay, Canada, 2010.