Model-Driven Approach for Privacy Management in Business Ecosystem

Feltus, Christophe; Grandry, Eric; Kupper, Thomas; Colin, Jean-Noël

Published in:
MODELSWARD 2017 - Proceedings of the 5th International Conference on Model-Driven Engineering and Software Development

DOI:
10.5220/0006142203920400

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Model-driven Approach for Privacy Management in Business Ecosystem

Christophe Feltus[1], Eric Grandry[1], Thomas Kupper[1,2] and Jean-Noël Colin[2]
[1]*Luxembourg Institute of Science and Technology (LIST), IT for Innovative Services (ITIS), Esch-sur-Alzette, Luxembourg*
[2]*Faculty of Computer Science (PReCISE), University of Namur, Namur, Belgium*

Keywords: Privacy Metamodel, Privacy Management, GDPR, General Data Protection Regulation, Business Ecosystem, Interconnected Society, Model, Service System, Model-driven Approach, Model Design.

Abstract: Protection of individuals with regard to the processing of personal data and the free movement of such data constitutes new challenges in terms of privacy management. Although this privacy management ought to be conducted in compliance with national and international regulation, for now we observe that no solution, model or method, fully consider and integrate these new regulations yet. Therefore, in this paper, we propose to tackle this problem through the definition of an expressive privacy metamodel which aims to represent and aggregate the concepts that are relevant to define and to deal with privacy issues, at an organizational level. Secondly, we discuss how this privacy metamodel may support and may help understanding the management of the privacy in enterprises involve in interconnected societies, by integrating the privacy metamodel with the systemic business ecosystem.

1 INTRODUCTION

Among the many challenges related to the privacy management is the protection of individuals with regard to the processing of personal data and the free movement of such data. This privacy management should be conducted by considering the arising dedicated national and international regulation and more especially, in Europe, the General Data Protection Regulation (GDPR) that is puts forward by the Regulation of the European Parliament and of the European Council. At the business level, the Ipswitch survey (Ipswitch, 2015) on 316 European companies reveals that 52 percent of the respondents estimate that they are not ready for applying the GDPR, and that 56 percent did not even know exactly what GDPR is. Only 12 percent feel ready to be compliant with it. A reason for this is that, at the present day, no solution (i.e. model, method, or tool) fully considers and integrates this new regulation yet. Simple and adapted approaches are by the way required to support information system designers to apprehend the GDPR and its impact on the whole business organization and business ecosystem. In that regard, we propose, in this paper, to set forth preliminary theoretic researches to define an expressive privacy metamodel (PMM) which allows representing and aggregating in an extended metamodel all the concepts necessary to define and to deal with privacy issues, at an organizational level. This metamodel is designed in compliance with Service System Theories (SST, Alter, 2011) and in the frame of a design (Hevner et al., 2004, Peffers et al., 2008) science approaches, including iterative cycles of literature review/model design/validation. Afterwards, to analyse and to depict the privacy management in the frame of interconnected societies (Cholez et al, 2014), we integrate the PMM with the business service ecosystem model and we discuss how the comprehension of the systemic privacy management may be improved on the basis of a model-driven approach. Finally, we illustrate the advantage of this integration into a case study from the Luxembourgish financial sector.

At a methodological level, the research that we tackle through this paper concerns the improvement of the alignment between the information processed by the information system and the management of the privacy, as required by the literature and by specific legal requirements, such as, mainly the GDPR. Through this research, we aim to strengthen the organizational capability to manage the access to

Feltus C., Grandry E., Kupper T. and Colin J.
Model-driven Approach for Privacy Management in Business Ecosystem.
DOI: 10.5220/0006142203920400
In *Proceedings of the 5th International Conference on Model-Driven Engineering and Software Development (MODELSWARD 2017)*, pages 392-400
ISBN: 978-989-758-210-3

sensitive and private information by enhancing the latter's ability to apprehend privacy and to comply with privacy requirements. At the methodological level, Hevner et al. (2004) explains that the Design Science Research (DSR) paradigm seeks to extend the boundaries of human and organization capability by creating new and innovative artefacts. Practically, provided that we aim to design a new artefact to support the alignment between private information and the management of the latter with the objective to grant the appropriate access rights to the users of this information, we acknowledge that the research may plainly be considered in the scope of DSR, as expressed in Peffers et al. (2008). As advocated by the DSR theory, the metamodel is built following an iterative approach. The latter allows refining a consistent privacy metamodel based on the review of the scientific literature and on the analysis of the privacy regulation.

The paper first proposes a review of the literature related to the privacy and depicts the related regulation Section 3 explains the design of the PMM and integrates it with systemic approach. Section 5 presents a case study from the financial sector. Finally, Section 6 discusses how it contributes in sustaining systemic privacy management, and Section 7 concludes the paper and proposes some future works.

2 LITTERATURE REVIEW

This section reviews the scientific literature related to privacy and the legal requirement from the GDPR.

2.1 Scientific Contribution

As explained in De Capitani di Vimercati et al. (2012), several definitions of privacy have been proposed over the years, from traditional syntactic privacy definitions to more recent semantic privacy definitions. In this paper, we consider privacy as *sensitive information that is individually owned* (Nuseibeh, 2010). The privacy management includes many aspects like the definition of privacy policy, the expression of the policy with a dedicated language or the execution of the latter with dedicated mechanisms. At a modelling point of view, privacy has often been addressed in parallel and as an extension of the access rights models (Park et al., 2000, Ni et al., 2007). For instance, Ardagna et al. (2008) analysed the concepts and features that should be investigated to fulfil the development of powerful and flexible privacy-aware models and languages. Privacy has been considered through the lens of the purpose associated to the usage of personal information. In that regards, a first model proposed by Antón et al. (2007) was UCON (Usage Control) which gathered in a single model the traditional access control models, the trust management and the digital rights management. In contrast to traditional access control models that control the access to an information in a unique direction (for instance, from the eCommerce site to the customer), UCON allows controlling the access at both sides and, hence, allows a user to control the information provided to the eCommerce website, which as a result guarantees the privacy to this information.

Park et al. (2002) explains that individual policies for each user's activity and for the use of each resource are similar to subject and object attributes and that the mutability of these attributes allows the continuity of decision (e.g. if a usage is no longer necessary, the access right is removed). In Martinez-Balleste et al. (2013), a framework is proposed to exploit the notion of privacy awareness requirements in order to detect runtime privacy properties to be satisfied. The latter are exploited to support disclosure decisions made by the applications. In Park et al. (2000), the Role Based Access Control (RBAC) model has been extended to provide support for expressing privacy policies (PRBAC) by considering at the same time users' purposes and obligations. Providing the system to protect customer privacy in mobile applications is a challenging task (Mahmoud et al., 2005). In Domingo-Ferrer et al. (2007), the author expresses that new development methods are necessary to enable the engineering of privacy specific requirements and proposes to extend the PRBAC model to reason about scenarios that potentially exploit mobile systems weaknesses (Martinez-Balleste et al., 2013). More recently, OrBAC has been semantically enriched to model privacy policies. The enhancement consists in considering the concepts of consent, accuracy, purposes of the access and provisional obligation (Ni et al., 2007). Ajam et al. (2013) analyse how OrBAC and PRBAC are adapted to address security issues in the healthcare sector and observes, amongst others, (1) that OrBAC is not adapted for managing the privacy regarding some roles (like the legal representative and the trusted person) given that a user must be strictly attached to an organization, and (2) that PRBAC fits well with the requirements of the information system from the healthcare regarding the patient's records (Ajam et al., 2013).

Rath et al. (2012) addresses privacy through the purpose of the access and proposes a model for

purpose enforcement. Accordingly, the authors also propose a system architecture that contributes to the enforcement of access purpose. In the field of privacy in social network circles, Rath et al. (2013) observe that existing privacy approaches are still not able to deal with the user's changing information sharing privacy requirements. This motivates the design of a utility-based trade-off framework which models and quantifies users' requirements and, based on it, appraises the potential privacy risks, on one hand, and the incentive social benefit, on the other. Regarding the organization more closely, Merriam (2016) has proposed a framework to address the database privacy according to three independent privacy dimensions: the respondent privacy (the entity to which the data collected corresponds), the user privacy (the entity that uses the data or makes queries in the database), and the owner privacy (the entity that owns the data). Using this framework, Merriam (2016) assesses the existing privacy enabling technology and observes that none of them allow fulfilling the three privacy dimensions at the same time.

The risk in revealing a user identity via location information has been formally introduced by Bettini et al. (2005) who present preliminary ideas about algorithms to prevent this to happen. More recently, Yang et al. (2014) propose a W3-privacy method to address the Location-Based Services (LBS – Service required by mobile devices with self-location capabilities). This method concerns the user privacy, according to the model from Merriam (2016), and is based on density maps (where the user identification is made uncertain due to the great number of users). Three elements of a service request are considered by W3-privacy: *Where the request is done?*, *What is requested?*, and *Who makes the request?*. Using the database privacy framework [4] and the LBS privacy method from Yang et al. (2014), Pérez-Martinez et al. (2011) propose a 5D citizens' privacy model for smart cities. The five privacy dimensions concerned by the model are the identity privacy (identity of the user of a service), the query privacy (query made by the user), the location privacy (the place where the query is done), the footprint privacy (information retrieved from sensors), and the owner privacy (equivalent to the definition of Merriam (2016).

2.2 GDPR

The General Data Protection Regulation (GDPR) is a Regulation which has for objective to strengthen and to unify, within the European Union, personal data protection and the export of such data outside the EU borders. The GDPR aims to replace the data protection directive 95/46/EC (DP, 1995) from 1995. Based on the deployment of the GDPR, it is expected to pass back the control on the usage of their personal data to European citizens. According to the European Commission, personal data is "*any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address*".

The GDPR lays down a set of rules with regard to the processing and related to the free movement of personal data. Hence, GDPR is to be read more as a regulation for the management of the privacy than for its definition. Accordingly, GDPR is more related to the concepts of privacy management (in light grey in Figure 5). The review of the articles of the GDPR which are relevant for the definition of the PMM has allowed capturing the following set of requirements necessary to be considered, in Table 1.

Table 1: GDPR principles and requirements about personal data.

Art.	Description
5a	Processed lawfully, fairly and in a transparent manner in relation to the data subject
5b	Collected for specified, explicit and legitimate purpose
5c	Adequate, relevant and limited to the minimum necessary
5d	Inaccurate must be erased or rectified
5e	Data subject to be identifiable for no longer than necessary
5f	Controller must ensure the compliance with the regulation
6.1a	Data subject gives consent to the processing and has the right to withdraw his/her consent
6.1b to 6.1d	Data processing is necessary for performance of a contract, legal obligation, vital or public interest, legitimate interests pursued by a controller

3 PRIVACY METAMODEL

The privacy metamodel (1) is structured according to three of the core concepts that compose the SST (Alter, 2011), i.e., the *Resource*, the *Role*, and the *Activity* and (2), based on the review of the state of the art summarized in Section 2, the metamodel is extended to the *Privacy management*. Concretely, during the elaboration of this first iteration of the metamodel, each relevant element from the review of

the state of the art (scientific contributions and GDPR) is introduced in the metamodel. In order to give an exhaustive view on the latter, and to allow traceability during the design step, a reference to the source of the relevant argument is introduced directly in the model, aside the concept's class name or the relation name between concepts, in brackets.

Concerning the GDPR, for accuracy reasons, a reference is directly done to the specific article which provides the requirement. E.g. the reference (GDPR A6.1b) is to be read: Article 6, point 1, sub-item (b). It is worth to mention that not all the components of the privacy are represented in this version of the metamodel. Some concepts and some relations have been omitted for preserving the readability. This metamodel has been modelled in UML 2.0 (Rumbaugh et al., 2004) and cardinalities have been removed.

3.1 Resource Related Concepts

The resource domain (Figure 1) represents the set of elements which are used by activities (Alter, 2011), e.g., participant, technology or information. The privacy of the information relates, as a result, to the privacy of a type of resources. This information supports *the representation of knowledge, what signifies understanding of real things or abstract concepts* (OPL). It may be of a sensitive type when it concerns personal data (Nuseibeh, 2010) such as a picture, a mail address, a physical characteristic of an individual, etc. In turn, a subset of this sensitive information may be an information which is relevant for a specific business and in that regard, limited to the minimum necessary to be collected and exploited by the information system (Zhu et al., 2007, GDPR A5c).

The concept of sensitive information is introduced and represented as a class in the privacy metamodel. It is of the type "resource" on Figure 1.

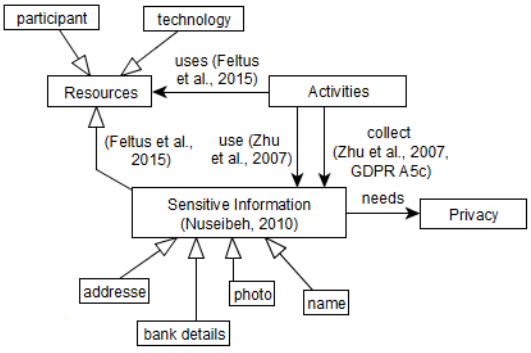

Figure 1: Resource sub-model concepts.

3.2 Role Related Concepts

The role domain gathers a set of roles having responsibilities in the management of the privacy, i.e., the *information owner*, the *controller*, the *information user*. The information owner is the actor who is legally accountable for the protection of the information collected. Hence, it is his responsibility to decide when and how information may be released or made available for processing. He is also called the data collector (Merriam, 2016) and corresponds to the individual or institution with which there exists a trust relationship with the information respondent. It may correspond to a person or to an institution, like for instance, a hospital, a bank, or a book-keeper. The controller must guarantee transparent and easily accessible information on the protection of personal data and privacy as well as the procedures for the *data subject* to fulfil its rights (GDPR). The controller must keep the information owner informed about the data manipulation (GDPR A14). The information user corresponds to an entity being able to compute queries across the databases in such a way that only the results of the query are revealed (Merriam, 2016). The information user corresponds to the "processor" in the GDPR. Moreover, Art. 26 of the GDPR stresses the fact that in case of a processor that processes data upon request of the controller, the processor must be associated to a joint controller.

This statement has not been modelled in the privacy metamodel for the sake of clarity. According to the GDPR, both the controller and the information user are responsible to set up the appropriate protection of the data. Moreover, roles are played by actors. A specific one of them is the data subject.

The data subject (GDPR) is the entity to which the information records correspond (Merriam, 2016). It is for instance the patient in a hospital or the customer of a bank. The data subject is allowed to give or withdraw his consent on the usage of personal information (GDPR A6.1a) and this usage must be transparent for him (GDPR A5a). Finally, Yang et al. (2014) also claims that the location where the actors

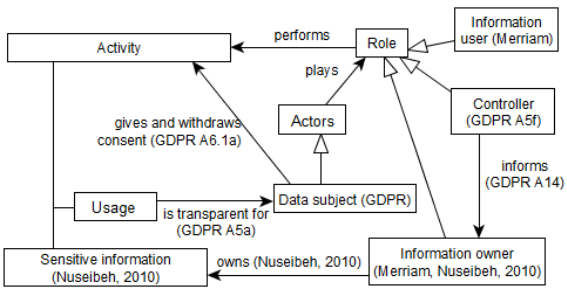

Figure 2: Role sub-model concepts.

operate is also a privacy parameter to be considered.

At the modelling level (figure 2), we have represented the concept of *Role* and *Actor* as classes. The first is played by the second. The concepts of *information owner*, *controller*, and *information user* are specializations of the class *role*, and the *data subject* is a specialization of the class *actor*.

3.3 Activity Related Concepts

In the frame of the Service System Theories (Alter, 2011), the *activity* is an element contains by the *organization* that produces services using *resources*. The *privacy management* is a type of activity which aims to support the information owner in performing the activities related to the administration of private data. The privacy management domain consists mainly in three activities: the *definition of the privacy policy*, the *enforcement of the policy*, and the *audit of the policy* (Ashley et al., 2003). The management of the privacy is performed in compliance with the *privacy policy*. This policy provides requirements in the way of how the privacy of personal data must be preserved and managed, in a company, while remaining in turn compliant with the appropriate legislation. This privacy policy determines the minimum needed and relevant information (Zhu et al., 2007, GDPR A5c) necessary to achieve a task and is applicable at all stages of the privacy management, to know: the collecting, the usage, the update, the disclosure and the erasure of the information. The three most important activities of the privacy management, according to Ashley et al. (2003), are the specification of privacy policies, their enforcement and the audit of their deployment.

The specification of the privacy policy aims at establishing the general and specific goals, as well as the procedures necessary to fulfil these goals. These privacy policies are adopted by the controller (GDPR A5f). The activity related to the enforcement of the policies corresponds to the achievement of procedures for the privacy management, either manually or with the support of the information system. The access rights, to the information system, represent hence a huge part of the means necessary for granting, or not, access to the information [8], and more especially, the minimum necessary and relevant information (Zhu et al., 2007, GDPR A5c). In that regard, the audit of the privacy policy concerns both: (1) that access rights/authorization are/is deployed in compliance with the privacy policy (Antón et al., 2007) and (2) that the latter is provided in accordance with the usage of the private data (Antón et al., 2007).

At a modelling point of view, the *privacy policy* and the *privacy management* concepts have been introduced as classes in the metamodel. The latter is a type of activity in the SST, it supports the information owner in fulfilling its responsibilities and is composed of the three explained activities here above, i.e. the *definition of the privacy policy*, the *enforcement of the policy*, and the *audit of the policy*.

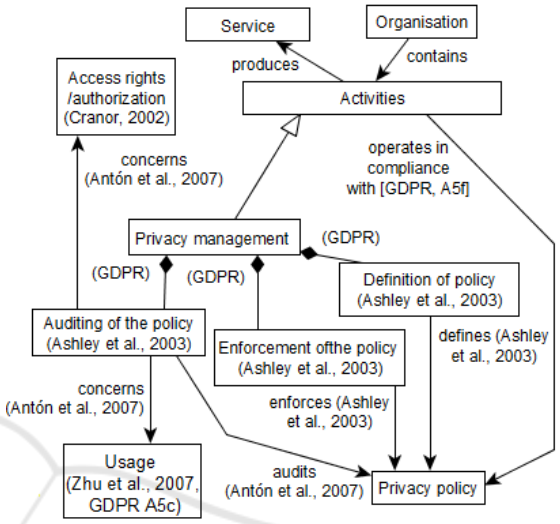

Figure 3: Activity sub-model concepts.

These concepts are also modelled as classes and the latter compose the privacy management class (actors and activity domains are represented in light grey in Figure 5).

3.4 Privacy Related Concepts

The Privacy extension domain supports the definition of *privacy* in function of the *usage* (Antón et al., 2007) made with the information and in function of the actors who manipulate the latter (Yang et al., 2014, Pérez-Martínez et al., 2011). As reviewed in literature and more especially in the GDPR, the usage concerns the information which is relevant for the business, to which access rights must be restricted to the minimum necessary (Zhu et al., 2007, GDPR A5c), and for which a purpose is clearly defined (Antón et al., 2007, GDPR A5b, A6.1b to d).

This purpose must be included in a list of well-defined purposes, expressed in the GDPR, e.g., for the performance of a contract of which the information respondent is part, for compliance with some legal obligations, in order to protect the vital interests of the information respondent, to carry out a task of public interest or in exercise of an official authority, or for a legitimate interest pursued by the controller. At a modelling point of view, the class *privacy* and the

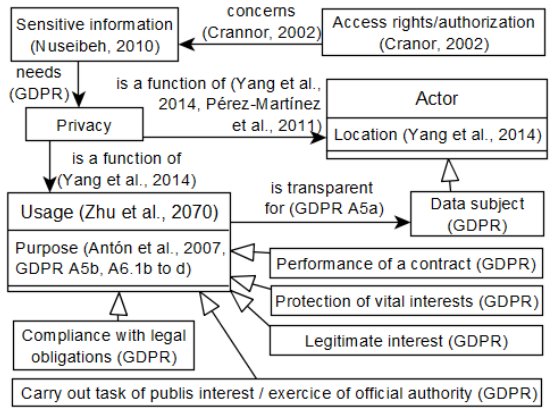

Figure 4: Privacy sub-model concepts.

relation class *usage*, that influences the need of privacy, have been modelled. In order to model this usage depending on the purpose, in the metamodel, we consider that this purpose is a type of attribute of the usage class (Figure 4).

3.5 Integrated Privacy Metamodel

Figure 5 presents the integrated PMM gathering the concepts from the resources, role, activity and privacy sub-domains. This integration allows establishing hyphens between concepts from all sub-domains, amongst which, e.g. the tasks and the actors/roles. The most important one is that the activity of a type *Privacy management* main objective is to support (Zhu et al., 2007) the *information owner* which has to *declare the (usage) intention* (Zhu et al., 2007) related to the *sensitive information* and to keep the latter up to date (GDPR A5.5e) (to know: *erase or rectify*). Aside the information owner, *Controller* defines (GDPR A5f) and audits (Antón et al., 2007) *privacy policies,* and *Information user* exploits *resources* in compliance with *access rights* and *authorizations*.

4 SYSTEMIC PRIVACY

This section give insights into the management of privacy at systemic level based on a model driven approach. Business ecosystems gather enterprises which collaborate to achieve a common systemic goal like guaranteeing national healthcare (Feltus et al., 2014), telecommunication (Wang et al., 1998), or financial stability (Naudet et al., 2016). A metamodel, named Business Service Ecosystem (BSE), was proposed (Feltus et al., 2016) to model these business ecosystems based on capabilities and resources (Figure 6). The BSE purpose is to represent how the resources of the business ecosystem are derived from the business ecosystem enterprises capability. We observe that two mappings exist between the PMM and the BSE. First, the resource from the BSE, at the business ecosystem or at the enterprise level, which is defined as *an asset that an organization has or can call upon*, is mapped with the resource from the privacy metamodel that refers to the SST (Alter,

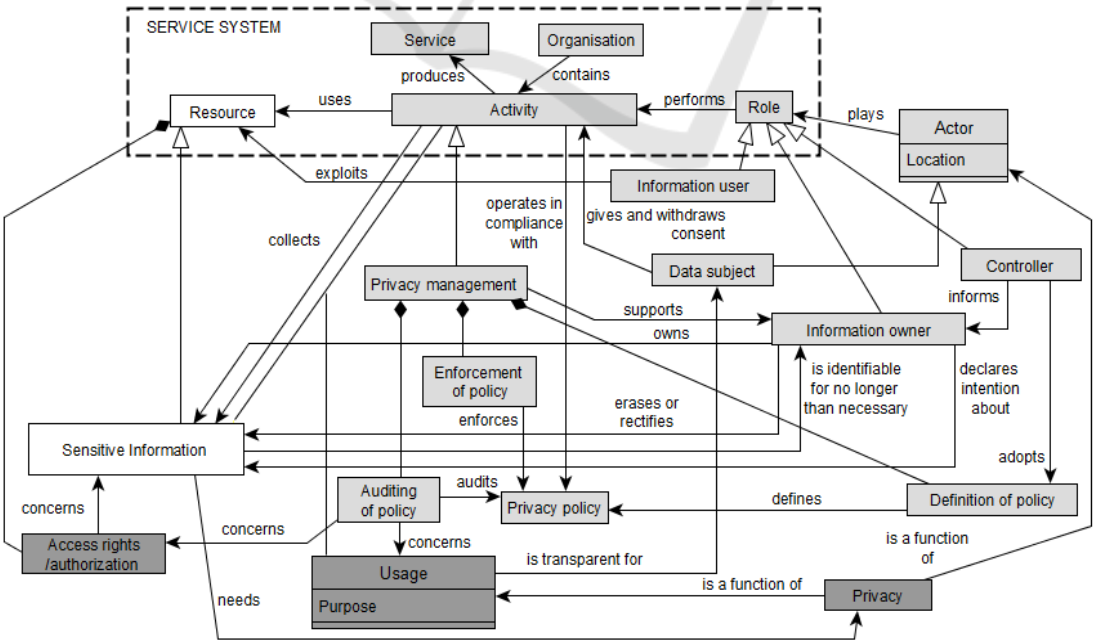

Figure 5: PMM. White concepts relates to resource, light grey to role and activity, and dark grey to the privacy extension.

2011) and which is defined as *participants, technological entities, informational entities, and other resources used by activities*. Second, there is an exact equivalence between the service definition from PMM (SST definition) and the service definition from BSE: "*acts performed for others, including the provision of resources that others will use*".

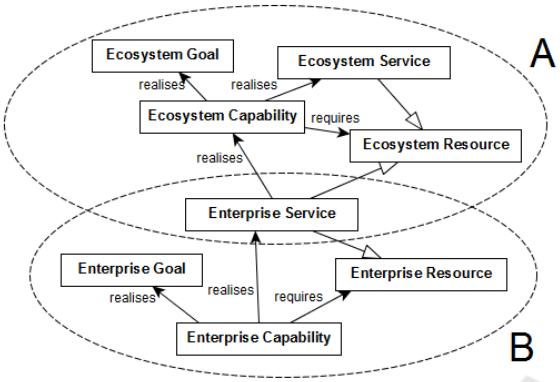

Figure 6: BSE metamodel, extracted from [28]. Pattern A corresponds to the business ecosystem and B to the enterprise.

At the systemic level, we have demonstrated in [28] that (1) an enterprise service (pattern B) is a type of business ecosystem resource (pattern A) and (2) the capability, which is defined as "*the ability and capacity that enable an enterprise to achieve a business goal in a certain context*" [26] is necessary to realize an enterprise/systemic service.

8 DISCUSSION AND CONCLUSION

In this paper, we have elaborated a PMM from a review of scientific privacy literature and from requirements from the GDPR. This metamodel is structured following the SST and allows structuring the management of the privacy at the enterprise level by defining privacy management services, supported by dedicated capabilities and specific roles. Afterwards, the privacy metamodel has been integrated with the BSE to extend the usage of the PMM to the context of enterprise working in the frame of interconnected societies.

Many approaches have been proposed to tackles privacy issues at the enterprise level (Section 2). However, as far as our knowledge goes, none of them has ever proposed an integrated metamodel for representing the many dimensions of the privacy, especially in compliance with the GDPR. In that regard, the first part of the paper has proposed the privacy metamodel built on existing theories and legal requirements. Aside our developments, we have also observed that in an interconnected societies and sharing economy context, managing the privacy at the enterprise level is far to be sufficient, and that new approaches are required to raise the privacy management from the enterprise boundaries up to the business ecosystem level. To answer this arising business requirement, we have proposed in Section 4.2 to integrate the PMM with the business service ecosystem. Afterwards, to assess the relevance and accuracy of the privacy metamodel in interconnected societies, we have evaluated the deployment of this artefact in the frame of substantive instances through a real financial case study. The latter has demonstrated that if we consider that the PMM structures the requirements for a compliant management of the privacy at the enterprise layer, it is also relevant to instantiate the concepts of this metamodel in order to apprehend and thus to manage privacy issues at the business ecosystem level. Based on the mapping with the BSE, we observe first that in order to manage the privacy (which may be perceived as a new type of service), the enterprise is required to develop new capabilities, respectively: to define privacy policy, to enforce the latter and to assess their enforcement. These capabilities also requires specific resources, e.g., some employees need to be affected to new privacy management roles like the information user, the controller or the information owner. New tools also need to be acquired to support the performance of Privacy Impact Assessment and access rights management. At the business ecosystem level, our analysis reveals that the same instantiation is necessary, although it sounds to be much trickier. Indeed, in this case, privacy management needs to be handled by a business ecosystem authority like, for instance in the case of the CSSF. The latter needs to analyse the systemic capabilities and resources required to realize systemic privacy services (business ecosystem service) in a service system environment. This context, justifies the need for the model-driven approach that we propose and which sustain the abstraction of the information system at the right level to support systemic privacy management. In regard to this evolution, we also observe the arising of new type of specific businesses to manage the systemic privacy (other type of business ecosystem services). These arising services in turn necessitate business ecosystem capabilities and resources such as dedicated systemic privacy management role, tools, and policies. A particular resource in this context concerns the Privacy Impact

Assessment methods. Various initiatives emerges to extend the use of risk assessment to the privacy domain. E.g., the *Commission nationale de l'informatique et des libertés* (CNIL - In English: *National Commission on Informatics and Liberty*) proposes a privacy risks assessment method, which can be integrated in a privacy impact assessment (Netha, 2016). The *National Institute of Standards and Technology* (NIST) is also developing a specific privacy risk management model and framework and attempting to integrate it with its security risk management framework. These initiatives can be seen as an extension to the Australian National eHealth Security and Access Framework approach (Netha, 2016), as they do not only address the CIA triad, but additional objectives associated with privacy. As the privacy objectives of the individuals are translated into objectives of the organization, they however remain focalized on fully assessing the risks (the combination of both threat and impact) on the organization. The PMM, as an extension of the SST, is an artefact that could sustain the PIA management. Therefore, the preliminary work related to the mapping between the risk and the BSE could serve as a good basis considering that risk of enterprise privacy breach is a function of the tuple privacy threat, privacy impact, privacy vulnerability. Based on the integration of BSE - PMM, and given the alignment between the risk concepts and the BSE, it is possible to extrapolate the enterprise PIA to the sectorial level as well.

REFERENCES

Ajam, N., Cuppens-Boulahia, N., Cuppens, F., 2013. Contextual privacy management in extended role based access control model. *DPM'13.* Springer.

Alter, S., 2011. Metamodel for service design and service innovation: *Integrating service activities, service systems, and value constellations.*

Antón, A.I., Bertino, E., Li, N., Yu, T. 2007. A roadmap for comprehensive online privacy policy management. Commun. *ACM 50(7*), pp. 109-116.

Ardagna, C. A., Cremonini, M., De Capitani di Vimercati, S., Samarati, P. 2008. *A privacy-aware access control system. Journal of Computer Security, 16(4), 369-397.*

Ashley, P., Hada, S., Karjoth, G., Powers, C., Schunte, M. 2003. *Enterprise privacy authorization language, 1.2.*

Bettini, C., Wang, X. S., Jajodia, S. 2005. Protecting privacy against location-based personal identification. *SDM 2005. p. 185-199.*

Cholez, H., Feltus, C., 2014. Towards an innovative systemic approach of risk management. *In 7th ACM SIN conference.*

CNIL, http://www.cnil.fr/fileadmin/documents/ en/ CNIL-PIA-1-Methodol ogy.pdf.

Cranor L., 2002. *Web privacy with P3P.* O'Reilly Media.

CSSF, 2012. Circulaire CSSF 12/544, *Optimisation of the supervision exercised on the "support PFS" by a risk-based approach.*

De Capitani di Vimercati, S., Foresti, S., Livraga, G., et al. 2012. Data privacy: definitions and techniques. *IJUFKS, vol. 20, no 06, p. 793-817.*

Domingo-Ferrer, J., 2007. A three-dimensional conceptual framework for database privacy. *4th VLDB, SDM'07.*

DP, 1995. data-protection/document/review2012/com_2012_11_en.pdf.

Feltus, C., Nicolas, D., Poupart, C., 2014. Towards a HL7 based Metamodeling Integration Approach for Embracing the Privacy of Healthcare Patient Records Administration. *7th ACM SIN conference.*

Feltus, F., Fontaine, F.-X., Grandry, E., 2015. Towards Systemic Risk Management in the frame of Business Service Ecosystem, *ASDENCA 2015.*

GDPR, Council of European Union. 269/2014. http://ec.europa.eu/justice/

Hevner, R., March, S. T., Park, J. 2004. Design science in information systems research. *MIS 28(1).*

Ipswitch, 2015, http://www.ipswitch.com/blog/european-teams-woefully-underprepared-gdpr/

Mahmoud, Y., Atluri, V., Adam, N. R., 2005. Preserving mobile customer privacy: an access control system for moving objects and customer profiles. *Mobisys, ACM.*

Martinez-Balleste, A.; Perez-Martinez, P.A.; Solanas, A. 2013. The pursuit of citizens' privacy: a privacy-aware smart city is possible*, IEEE, 51(6), pp.136-141.*

Merriam, 2016. http://www.merriam-webster.com/ dictionary/information.

Naudet, Y., Mayer, N., Feltus, C., 2016. Towards a Systemic Approach for Information Security Risk Management*, ARES 2016. IEEE,* Austria.

Nehta, https://www.nehta.gov.au/implementation-resources/ehealth-foundations/ national- ehealth- security -and-acc ess-framework.

Ni, Q., Trombetta, A., Bertino, E., Lobo, J. 2007. Privacy-aware role based access control. *SACMAT '07, ACM.*

NIST, http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_dra ft.pdf.

Nuseibeh, B., 2010. Mobile privacy requirements on demand. *In PROFES 2010.* Springer.

OPL, Online Privacy Law: European Union, http://www.loc.gov/law/

Park, J., Sandhu, R. 2002. Towards usage control models: beyond traditional access control*. SACMAT '02. ACM.*

Park, J., Sandhu, R. 2000. A position paper: a usage control (UCON) model for social networks privacy.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2008. A design science research methodology for information systems research. *JMIS 24(3):45-77.*

Pérez-Martínez, P.A., Solanas, A. 2011. *W3-privacy: the three dimensions of user privacy in LBS, Int'l. Symp.*

Rath, T.M.A., Colin, J.-N., 2012. Patient privacy preservation: P-RBAC vs OrBAC in patient controlled records type of centralized healthcare information

system. *Case study of walloon healthcare network. eTELEMED.*

Rath, T.M.A., Colin, J.-N., 2013. *Towards enforcement of purpose for privacy policy in distributed healthcare. CCNC.* IEEE.

Rumbaugh, J., Jacobson, I., Booch, G. 2004. Unified Modeling Language Reference Manual, The. *Pearson Higher Education.*

Wang, H., Lee, M. K., & Wang, C. 1998. Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41(3), 63-70.*

Yang, M., Yu, Y., Bandara, A., Nuseibeh, B. 2014. Adaptive sharing for online social networks: a trade-off between privacy risk and social benefit. *TrustCom-14*.

Zhu, Y., Peng, L. 2007. Study on K-Anonymity Models of Sharing Medical Information. *ICSSSM 2007. IEEE.*