E-Government and On-line Services: Security and Legal Patterns

Paolo Guarda[1], Fabio Massacci[2], and Nicola Zannone[2]

[1] Department of Legal Sciences
University of Trento, Italy
paolo.guarda@unitn.it

[2] Department of Information and Communication Technologies
University of Trento, Italy
{massacci,zannone}@dit.unitn.it

E-government refers to the introduction of digital technologies into public administrations and it is assuming a pivotal role in many countries, including Italy. In particular, the supply of on-line services by public administrations represents a rapidly expanding phenomenon. The objective of the paper is to support system designer in the development of IT systems that comply with regulations that govern the use of technologies in public administrations. Thus, taking as running example a tax portal and its authentication issues, we look at the general principles and rules that govern institutional sites and portals, as established in the Italian Public Administration Code. We also show how Security Requirements Engineering methodologies can assist system designers in their activities.

1. – Introduction

Public administrations are increasingly involved in the distribution of Information and Communication Technologies (ICT) and it is assuming the role of leader actor and promoter of the information society [1,2,3]. Nowadays, public administrations are one of the most important producers of information, collected for specific purposes related to public functions; they are also promoters since they have to establish the rules that govern the supply of (public or private) services of information to the citizens and to incentive the use of the digital technologies by citizens [4].

The European Union defined e-government as "the use of information and communication technologies in public administrations combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies" [5]. Thus, this definition involves the electronic (or digital) civil service, i.e. all the deeds aimed to simplify the activity and the organization of the civil service itself in order to provide better services to citizens, as well as **"**eDemocracy", i.e. the deeds aimed to make more transparent and participated the public administrations actions.

According to the above definition, e-government should consider the perspective of citizens and users, since it has to represent the point of reference for every transformation process of public administrations. The main idea is that the spreading of ICT in public administrations and in the society has, in general, to be leaded by public purposes and goals, rather than by the sectoral trend of technology development.

It is possible to identify four dimensions of e-government:

1) a internal dimension of every public administration that uses ICTs, which concerns the re-organization of offices, processes, and competences;

2) an internal dimension of the public sector in general, which concerns the development of network interconnecting different public administrations;

3) an external dimension, which involves the relationship with private sectors;

4) an external dimension, which concerns the relationship between public administrations and citizens with respect to the provisioning of information.

1.1 Contribution of this paper

Our objective is to support system designers in the development of IT systems that comply with the regulations that govern the use of technologies in public administrations. The last years have seen an increasing interest in software engineering methodologies that address the problem of capturing security aspects from the early phases of the software development process. However, they are not founded on the general principles and rules set by legal systems. These recognize the pivotal importance of linking problems related to the diffusion and development of e-government to organizational issues.

In this paper, we analyze the Italian legal system concerning e-government matters. On the basis of this analysis, we show how Security Requirements Engineering methodologies can assist system designers in their activities. In particular, we adopt Secure Tropos [15], a requirements engineering methodology tailored to model functional, security and privacy aspects of socio-technical system. This framework is founded on the notions of ownership, provisioning, trust, and delegation in order to define entitlements, capabilities, and duties of stakeholders and system's actors and their transfer. There are evidence that above concepts are sufficient to model and analyze industrial case studies encompassing on ISO-17799 security management policies [19]. We have used Secure Tropos to analyze the impact of different protection mechanisms on the confidence of actors about the achievement of their objectives. In particular, we have analyzed identification issues of public portals as solved by the Italian "Public Administration Code".

The remainder of the paper is structured as follows. Section 3 presents the general principles defined by the Italian legal system to address e-government issues. Section 3 discusses security requirements for portals. Section 4 gives a brief overview of Secure Tropos and Section 5 shows how it can be used to model and analyze a Tax Portal. Section 6 discussed authentication issues of the Tax Portal. Finally, Section 7 concludes the paper.

2. - E-Government and administrative organization

2.1 – Development of e-government policies

The development of technologies for e-government can be divided in five periods:

1) The first period is characterized by the computerization of some administrative actions by single public administrations. The objective was to simplify such actions and reduce their cost by replacing human efforts with computer processing.

2) The second period is characterized by more general goals of public administrations, due to the increased capacity of processing data by ICTs. In this stage, we have a complete computerization of administrative actions.

3) In the third period, we find the problem of interconnecting the IT systems of different public administrations in order to share information and simplify data processing. Therefore, the problem was to build up an unitary network across different public administrations. However, this network was conceived as an Intranet network (i.e. not accessible by private citizens).

4) The fourth period is leaded by the diffusion of the Internet. The spread of new ICTs allows for new methods in order to share information, such as e-mails, Web-sites, and portals. This has also changed the focus of e-government: before the ICTs were conceived to improve the capacities of public administrations, now it is the citizen who assumes the pivotal role. In this setting, every point of the net can be seen as a *front office*, opened to external access, and the entire network constitutes a *back office* (all the data and information placed at disposal of everybody who accesses the net).

5) The fifth period is distinguished by a new attention on the contents and organizational impact of the computerization of activities and processes. It has been recognized that it is not sufficient to develop infrastructures and networks; public administrations also have to guarantee that they manage information with respect to the right level of quality and security.

2.2 - General principles and regulations of the different sectors

Initially, regulations for e-government were not systematic. To have a complete framework of e-government in the Italian legal system, one had to consider the administrative regulations of different sectors. There were rules regarding the automatized information systems of the public administrations [6]; rules on connectivity and interoperability [7]; rules on administrative documents [8]; rules on the right to access to the public records [9]; etc..

However, in the last years there was a new trend that tries to reorganize rules in a more complete and organic manner. The outcome was the Public Administration Code that has been enacted by means of d.lgs. March, 7, 2005, n. 82 [10]. The Code came into force on January, 1, 2006. Its main goal is to provide and ensure the availability, management, access, transmission, and conservation of the information stored by a digital medium [11]. It represents a sort of benchmark on the computerization of the Public Administration and e-government in general.

However, other general principles for e-government can be found in other statutes:

1. connection among the activities of different offices: local authorities shall be organized in order to assure the availability, the access, the communication of the informations in a digital format (see art. 2 (1)c [12]);

2. use of telematics: public administrations shall provide incentives for using telematics in order to improve the efficiency of the communication among different offices and between them and citizens (see art. 3-bis [9]).

3. - The On-line Services: Web-Sites and Portals

3.1 Definition. Access and availability of on-line information

The supply of on-line services by public administrations represents a rapidly expanding phenomenon. The Italian Public Administration Code does not define the services to be provided precisely. Rather, it provides a structured regulation that determines how they shall be provided [13].

The concept of Web-site refers to hypertext pages stored in a server and accessible from remote clients. The Public Administration Code establishes a specific regulation for public Web-sites. In particular, these shall be structured in order to provide information and services and to establish a community of users.

The notion of "institutional site" or "public administration site" assumes a specific meaning from a legal viewpoint. In particular, they shall comply with articles 53 and 54 [10]. According to art. 53 (1)c [10], Web-sites have to comply with several principles. Actually, it states that: "the central public administrations realize institutional sites on telematic network that fulfill the principles of *accessibility*, of high level *usability* and *availability*, also by people with disabilities, *completeness* of information, clearness as regarding the language, *dependability*, consultation *simplicity*, *quality*, *uniformity*, and *interoperability*". Among the others, *accessibility* means that public administrations have to implement the technologies necessary to guarantee the access to information and services also by people with disabilities. Another important principle is *usability* that requires that information and services have to be organized in a way that assures the maximum level of utilization. *Dependability* and *availability* refer to secure issues: the first concept is defined as the trustworthiness of the IT system; the second principle regards the degree to which a system is operable. Moreover, the disclosure of data is characterized by other requirements, namely *accuracy*, *integrity*, and *confidentiality* (see art. 51 [10]). These principles are the similar to those that can be found in data protection regulations.

The Code establishes also some mandatory contents of the institutional Web-sites: these contents are related to information about the organization with regard to the transparency as well as legal dispositions, competences in processing, and a complete list of institutional e-mail accounts.

The categorization of on-line services is manifold: financial and non-financial services, supplied to citizens and to companies; each of them has own specific features (health care, educational, bureaucratic services). It seems to be advisable to distinguish them with respect to the relation established with the citizen. For our purpose, we distinguish among services with informative content, participatory content, or transactional content. The latter services are critical since they allow for the completion of on-line activities and procedures. They represent a new frontier that leads to the creation of new dedicated sites, in addition to the institutional ones [14]. An example of these new portal is represented by the Tax Portal. These kind of portals are more and more used to simplify the interaction among citizens and public administrations, concerning the payment of taxes, bills, and fines.

In the supply of on-line services, public administrations aim to better satisfy users' needs and, in particular, to ensure the completeness of processes and the certification of results, as well as verify the level of user satisfaction (see art. 63 (2)c [10]). It follows that the correct

execution of transactions is possible only if suitable identification, authentication, signature, and forwarding methods are in place.

3.2 Identification problem

Depending on the service they offers, portals can be distinguished among portals that needs authentication services and portals giving free access. In particular, authentication services are necessary when there are interactions between users and portals. For instance, they are strongly required in presence of transactional services. On the contrary, if a portal only offers informative services, authentication services are not strictly necessary.

Though authentication services might be provided in different ways, the Public Administration Code (art. 64) enforces the use of the CIE ("carta d'identità elettronica": electronic identification card) and CNS ("Carta nazionale dei servizi": national services card). These are smart cards whose chips are designed to support digital signature. Actually, the CIE and CNS provide two main kinds of services: a) services that simply require a secure identification of the users, such as the on-line request of documents; and b) qualified services that strongly need the storage of information on the card, such as the blood group for health-care purposes.

According to the Code, this authentication method is mandatory from December, 21, 2007 (see art. 64 (3)c [10]). Until that time, public administrations can adopt different methods, such as PIN and password-id, to determine the identity of citizens.

4. – The Secure Tropos Methodology

To understand why, how, and where solutions to security problems have to be deployed, system designers must model the goals, assets and trust relationships of the stakeholders of the socio-technical system as a whole. Among various proposals, we have chosen Secure Tropos [15], an agent-oriented security requirements engineering methodology. The main advantage of these early requirements methodologies (as opposed to downstream modeling languages such as UMLSec [16] or SecureUML [17] is that one can capture not only the *what* or the *how*, but also the *why* a security mechanism should be introduced in the system.

The Secure Tropos methodology adopts the SI* modeling language [18] for the acquisition of requirements. This language allows designers to capture the requirements of organizations together with their IT systems in a number of graphical diagrams, namely

Actor Diagram describing objectives, entitlements and capabilities of each actor.

Trust Diagram describing the social relations between actors. In particular, this diagram represents the expectations of actors about the performance and fair behavior of other actors in terms of trust of execution and trust of permission.

Execution Dependency Diagram identifying the dependencies among actors and, in particular, to which actor the achievement of which goals, the execution of which tasks or delivery of which resources has been assigned by which actor.

Permission Delegation Diagram identifying the transfers of right among actors and, in particular, to which actor has been delegated the permission on which goals, tasks, or resources by which actor.

Each of above diagrams represents a view of the requirements model. In the graphical representation of this model, objectives, entitlements, and capabilities are represented using request (**R**), ownership (**O**), and provide (**P**) relations, respectively. Permission delegations are represented with edges labeled by (**Dp**) and execution dependency with edges labeled by (**De**). Finally trust of permission relations are represented with edges labeled by (**Tp**) and trust of execution relations with edges labeled by (**Te**).

From a methodological perspective, Secure Tropos is based on the idea of building a model of the system that is incrementally refined and extended. Specifically, goal analysis consist of refining goals and eliciting new social relationships among actors. They are conducted from the perspective of single actors using means-end analysis, AND/OR decomposition, and contribution analysis. *Means-end analysis* aims at identifying the tasks used to achieve a goal and the resources consumed and produced by a task. *AND/OR decomposition* combines AND and OR refinements of a root goal or a root task into subparts. In essence, AND-decomposition is used to define the high-level process to achieve a goal or a task, while OR-decomposition defines the alternatives to achieve a goal or execute a task. *Contribution analysis* identifies the impact of the achievement of goals and tasks over the achievement of other goals and tasks.

5. – Modeling a Tax Portal

This section addresses the on-line services that can be supplied by a fiscal administration. Every citizen may connect through Internet to the finance agency to process the tax declaration. At the same time, the finance agency can provide any document which can help a tax payer to use the application and to declare his incomes on the portal. Roughly speaking, the fiscal portal allows citizens to consult, compute, declare, and pay tax on-line as well as to get information by current fiscal event consultation and download documents and forms.

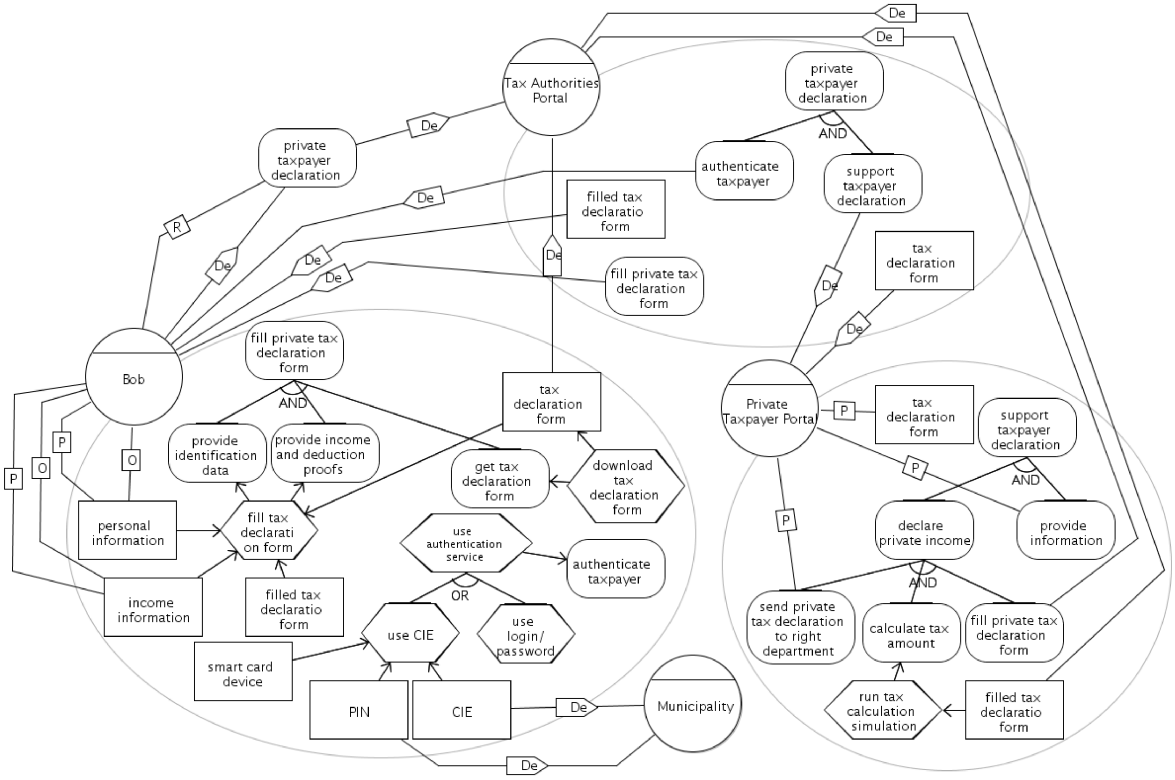
This scenario has been analyzed using Secure Tropos in the context of the SERENITY Project[1] for the definition of a Security and Dependability patterns library. In the remainder of this section we report the outcome of the modeling phases proposed by the SI* modeling framework to an excerpt of this study. We refer to [20] for the complete analysis of the domain.

The first activity in the requirements analysis process is actor modeling. Below the main stakeholders and system actors involved in the fiscal domain are analyzed along their objectives, entitlements, and capabilities.

> **Bob** is a private taxpayer, who wants to exploit the on-line tax service offered by the fiscal administration.
>
> **Tax Authorities Portal** is the tax portal entry point. It is responsible to provide information to taxpayer and provide access to on-line tax services, by connecting taxpayers to the dedicated portals.
>
> **Private Taxpayer Portal** is a dedicated portal that offers on-line tax services to private taxpayers, such as the consultation and management of personal tax space, the calculation of tax amount, and the on-line tax payment. Its main objective is to assist private citizens in tax declaration.

1EU-IST-IP 6th Framework Programme - SERENITY 27587 - http://www.serenity-project.org

The requirements modeling process proceeds by introducing the social relations between actors and the consequent integration of security and functional requirements. Figure 1 shows the graphical model representing the fiscal scenario.



Bob wants assistence for his tax declaration and accesses the Tax Authorities Portal for it. Before offering its services, the Tax Authorities Portal requires Bob to authenticate himself. The portal provides citizens with different authentication methods, namely using the CIE or using login and passord. In the case Bob uses the CIE for authentication purposes, he needs the electronic ID card and the corresponding PIN, for which he depends on the Municipality that is the government agency appointed to the issuance of electronic ID cards, and a smart card reader device. In the case Bob decides to authenticate himself using the user-name/password methods, the Tax Portal allows him to create user-names and passwords and requires a valid user-name and password to get in to the portal. To ensure a high-level security, the Tax Portal can force users to change their password after a certain time, let say every 2 months.

Once the user is authenticated, the Tax Authorities Portal forwards Bob's request to the Private Taxpayer Portal. The dedicated portal supports citizens in taxpayer declaration by providing them with the technical assistence for declaring private income and the information necessary to do it. To achieve its duties, the Private Tax Portal requires Bob to fill the private tax declaration form, for which the portal depends on Bob (via Tax Authorities Portal). The citizen downloads the tax declaration form from the Private Tax Portal and fills it by providing his indentification information as well as income information and deduction proofs.

Based on the tax deduction form filled by Bob, the dedicated portal calculates the private tax amount that Bob has to pay and sends the tax declaration form to the right department. Notice that the filled tax deduction form contains private information about the citizen. As consequences, the Tax Portal shall guarantee the integrity and confidentiality of such document. Moreover, the portal shall avoid that some malicious actor uploads a corrupt tax declaration form in behalf of legitimate actors. In this setting, authentication and, in particular, the selection of an adequate authentication method, play a fundamental role in the protection of citizens.

Finally, it is worth noting that there is not a direct link between Bob and the dedicated portal, but they inteact only through the Tax Authorities Portal. This requires to protect the integrity and confidentiality of the communications between the Private Taxpayer Portal and the Tax Authorities Portal, besides of the communications between the Tax Authorities Portal and the citizen.

6. – Authentication Issues

As described in Section 3, the introduction of ICT technologies in the public administration introduces a number of non-functional and security requirements that must be enforced by the public admnistration itsef. The implementation of security requirements have a strong impact on the trust of citizens towards the system and on the trust of public administration towards citizens, where trust is imperative for the successfully provisioning of on-line services to citizens. In the context of the Tax Portal, the confidentiality and integrity of data as well as the availability of on-line services 24 hours a day play a fundamental role. For instance, the fiscal administration shall guarantee citizens that only authorized users can access services provided by the agency as well as data contained in agency's databases since the fiscal administration handles very sensitive information.

Among security requirements, we mainly focus on authentication. The Tax Portal must be able to verify who is accessing services. If it cannot ensure that the party in the transactions is honest, the agency and citizens are at risk and, consequently, decreasing the trust on the portal. As shown in Section 3.2, public administrations can adopt different authentication mechanisms, and each of them can have a different cost and a different impact on the level of trust between the agency and citizens for the authentication process and on the confidence about identity and privacy protection that citizens feel towards the agency. Currently, the most used authentication methods are passwords and CIE.

Both these solutions have light and shadow. The use of CIE guarantees a higher level of security than the use of passwords. In particular, the use of CIE increases the trust in the authentication process, ensuring the financial administration about the identity of the citizen and citizens that malicious actors cannot upload documents in behalf of them. However, the cost of CIE is greater. Firstly, the public administration should build up a complex infrastructure involving new actors such as a Register Authority appointed to identify citizens by validating the information provided by them, a Certificate Authority appointed to issues digital certificates, and an Authentication Service Centre appointed to the management of certificates. Then, each citizen needs a smart card reader device in order to use the CIE for authentication purposes, besides the cost of the smart card itself. Moreover, the use of the CIE makes it easy to trace activities of citizens, so their privacy may be compromised.

7. – Conclusions

The widespread diffusion and implementation of e-government still presents some unsolved and problematic points. First of all, public administrations have difficulties in completing the computerization process since many documents are still collected in paper format.

Public administration shall also consider the importance of protecting and promoting the public information patrimony. To this end, it is necessary to computerize the whole documentation in every single public administration and then to integrate the IT systems of different public administrations.

Another problematic issue is represented by the necessity to protect the rights related to the development of ICTs. The new technologies allow a more pervasive protection of traditional and well established rights, as the right to access public records and the availability of information for the democratic control of the administrative activities. However, new rights are arising, namely the right to be informed, the right to privacy, and the right to effectively access personal information and systems that collect them (digital divide).

A fourth problematic point deals with the unclear relations between the right to access to the public records and the documents contained in, and the public transparency. We see a growing trend to reduce the right to access only to the cases in which one needs those documents to defend his legal positions, for instance in front of a court, while the digital technologies would allow you to reach a much more wide access to every information collected by the public administrations, opening the new way of a really democratic control of the citizens on the state actions.

Finally, we do not have an acquired awareness of inseparability among flow of information management processes and administrative re-organization processes yet. The traditional organizational solutions (allocation of competences among offices) have to be reconsider. On this point, e-government gives the chance for a review and reform of the administrative policies.

Acknowledgment

This work has been partially funded by EU Commission, through the SENSORIA and SERENITY projects, by the FIRB program of MIUR under the TOCAI project, and by the Provincial Authority of Trentino, through the MOSTRO project.

References

[1]F. Sarzana di S. Ippolito (edited by), “E-Government. Profili teorici ed applicazioni pratiche del governo digitale”, La Tribuna, Piacenza, 2003

[2]G. Vespertini (edited by), “L’e-Government”, Giuffrè, Milano, 2004

[3]F. Merloni, “Introduzione all’@Government. Pubbliche amministrazioni e società dell’informazione”, Giappichelli, Torino, 2005

[4]M. Bombardelli, Informatica pubblica, e-government e sviluppo sostenibile, in: Riv. it. dir. pubbl. comunitario, 2002, 991

[5]Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - The Role of eGovernment for Europe's Future (Com (2003) 1038))

[6]D.lgs. February 12, 1993, n. 39 "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm)", della L. 23 ottobre 1992, n. 421, Gazz. Uff. February 20, 1993, n. 42

[7]D.lgs. February 28, 2005, n. 42 "Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003, n. 229", Gazz. Uff. March 30, 2005, n. 73

[8]D.P.R. December 28, 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", Gazz. Uff. February 20, 2001, n. 42 (ordinary supp.)

[9]Statute August 7, 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", Gazz. Uff. August 18, 1990, n. 192

[10]D.lgs. March 7, 2005, n. 82 "Codice dell'amministrazione digitale", Gazz. Uff. May 6, 2005, n. 112

[11]M. Quaranta (edited by), "Il Codice della pubblica amministrazione digitale. Commento ragionato al Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche, Liguori, Napoli. 2006

[12]D.lgs. March 30, 2001, n. 165 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", Gazz. Uff. October 16, 2001, n. 241

[13] R.M. Di Giorgi, Reti di relazioni nella Pubblica Amministrazione. Considerazioni in tema di e-government e accesso alla documentazione di fonte pubblica, in: Informatica e dir., 2002, fasc. 2, 27

[14]CENSIS, Le Città digitali, Rapporto, available on the Web-site: http:\\www.rur.it

[15]P. Giorgini, F. Massacci, N. Zannone: Security and Trust Requirements Engineering, in: FOSAD 2004/2005, LNCS 3655, pp 237–272. Springer-Verlag, 2005

[16]J. Jürjens, "Secure Systems Development with UML", Springer-Verlag, 2004

[17]D. Basin, J. Doser, T. Lodderstedt, Model Driven Security: from UML Models to Access Control Infrastructures, TOSEM 15(1) 39–91, 2006

[18] F. Massacci, J. Mylopoulos, N. Zannone, An Ontology for Secure Socio-Technical Systems, in: Handbook of Ontologies for Business Interaction. The IDEA Group, 2007

[19] F. Massacci, M. Prest, N. Zannone, Using a Security Requirements Engineering Methodology in Practice: the compliance with the Italian Data Protection Legislation, in: Computer Standards & Interfaces, 27(5): 445-455, 2005

[20] Y. Asnar, R. Bonato, V. Bryl, L. Compagna, K. Dolinar, P. Giorgini, S. Holtmanns, T. Klobucar, P. Lanzi, J. Latanicki, F. Massacci, V. Meduri, J. Porekar, C. Riccucci, A. Saidane, M. Seguran, A. Yautsiukhin, and N. Zannone, "Security and privacy requirements at organizational level," SERENITY consortium, Research report A1.D2.1, 2006.