2016 IEEE 24th International Requirements Engineering Conference

Privacy Requirements: Findings and Lessons Learned in Developing a Privacy Platform

Mohamad Gharib*, Mattia Salnitri*, Elda Paja*, Paolo Giorgini*, Haralambos Mouratidis†,
Michalis Pavlidis†, José F. Ruiz‡, Sandra Fernandez§, Andrea Della Siria¶
* University of Trento, Trento, Italy
{mohamad.gharib,mattia.salnitri,elda.paja,paolo.giorgini}@unitn.it
† University of Brighton, Brighton, UK
{H.Mouratidis,M.Pavlidis}@brighton.ac.uk
‡ Atos, Madrid, Spain
jose.ruizr@atos.net
§ Bambino Gesú Children's Hospital, Rome, Italy
sandra.fernandez@opbg.net
¶ Business-e, Rome, Italy
Andrea.DellaSiria@business-e.it

***Abstract*—Information practices and systems that make use of personal and health-related information are governed by European laws and regulations to prevent unauthorized use and disclosure. Failure to comply with these laws and regulations results in huge monetary sanctions, which both private companies and public administrations want to avoid. How to comply with these laws, requires understanding the privacy requirements imposed on information systems. A holistic approach to privacy requirements specification calls for understanding not only the requirements derived from law, but also citizens' needs with respect to privacy. In this paper, we report on our experience in conducting privacy requirements engineering as part of a H2020 European Project, namely VisiOn (Visual Privacy Management in User Centric Open Requirements) for the development of a privacy platform to improve the interaction between Public Administrations (PA) and citizens, while guarding the privacy of the latter. Specifically, we present the process for eliciting, classifying, prioritizing, and validating privacy requirements for the two types of users, namely PA and citizen. The process is applied to different cases spanning from healthcare to other e-governmental initiatives, with the active involvement of the corresponding PAs. We report on findings and lessons learned from this experience.**

***Index Terms*—Privacy requirements; requirements engineering; elicitation; classification; prioritization; validation**

I. Introduction

Dealing with privacy is an important activity because privacy violations have severe repercussions spanning financial losses, legal exposure and compromising brand/reputation [1]. For instance, according to the HIPAA Privacy Rule [2], failing to protect the confidentiality of patients medical records, especially for commercial advantage or malicious harm, results in fines of $250,000 and imprisonment for up to 10 years. Moreover, several studies had shed more light on the economic costs of privacy breaches [3], making it clear that the absence of appropriate privacy protection mechanisms imposes huge expenses in the range of billions of dollars of losses as reported by [4]. A similar situation is seen in Europe, with new Privacy directives being approved by the EU Commission.

As such, privacy has become a main concern not only for private companies, but also for Public Administrations (PAs) and in particular those in countries moving toward the implementation of e-government [5]. Although a highly relevant activity, organizations still suffer from bad security practices, hacker and most importantly insider attacks, data thefts, etc. [3]. In order to ensure the desired privacy level, there is a need for a holistic approach to privacy requirements engineering, as advocated by Privacy by Design [6], [7].

Nevertheless, for decades information privacy has been treated as part of security ([6], [8], [9]), capturing mainly confidentiality, and overlooking aspects related to privacy assessment and verification to mention a few. Not only is this view limiting, it also treats privacy requirements as non-functional desired properties of a system. Other approaches either do not illustrate their practice with real experiences (using simulated examples), or propose solutions for the design of systems from scratch. But this is not always the case, since most systems today are developed by modifying and/or enhancing previous systems or components of systems [10].

Another trend is the work of Breaux et al. [11], which captures privacy requirements derived by law, overlooking user (citizen's) privacy requirements. The latter is quite important as demonstrated by [12], as citizens might refrain from using several services when their privacy is endangered. According to Spiekermann et al. [13] an increasing majority of US and EU citizens are worried about the level of privacy protection that services providers use while dealing with their private information. Thus, considering privacy may increase the citizens' trust in PAs, which increase their adoption of PAs services, and enable PAs to better perform their duties.

In this paper, we report on our experience in dealing with privacy requirements for a real world project, namely VisiOn (Visual Privacy Management in User Centric Open Environments), where we focus on the interaction between PAs and citizens. The particularity of Vision is that it gives citizens

2332-6441/16 $31.00 © 2016 IEEE
DOI 10.1109/RE.2016.13

RE 2016, Beijing, China
Industry Paper

a voice in specifying and capturing the privacy preferences, along those of the PAs as required by privacy norms. This inclusion makes a holistic approach to privacy requirements engineering, and is supported by a process for eliciting, classifying, prioritizing and validating the privacy requirements of two types of users (PAs and citizens) to be used for developing the VisiOn privacy platform. Specifically, PAs are used as the main source for defining the privacy requirements of the users that are responsible for managing the citizens' information, while citizens are used as the main source for defining the privacy requirements of information owners. Furthermore, we describe how the process has been used to analyze the VisiOn user requirements, and then we summarize our findings along with the lessons learned.

The rest of the paper is organized as follows; we describe the VisiOn project in Section II, while in Section III we present the process for eliciting, classifying, prioritizing and validating privacy requirements. Section IV discusses how the process has been used to analyze the VisiOn user requirements. In Section V, we present our findings and lessons learned while using the process for VisiOn user requirements. Finally, we conclude the paper in Section VI.

II. The VisiOn Project

PAs are working towards upgrading the level of their online services through new governance models such as the Open Government. This pushes for greater transparency, accountability and innovation aiming at increasing citizen levels of confidence and trust in PAs services. In this context, to improve citizens' acceptance of services provided by PAs, it is important to develop privacy-aware approaches that, on one hand allow citizens to understand their privacy needs and analyze them in the context of the various public services they might use, and on the other hand, enable PA departments to analyze and design services that take privacy into account throughout the development process.

With this in mind, the main aim of the VisiOn project[1] is developing VisiOn Privacy Platform (VPP) a user-centric privacy management platform for PAs and citizens. The VPP will enable the two types of its users (citizens and PAs) to understand their privacy needs, as well as identify and analyze how these needs comply with relevant laws and regulations.

The VPP will equip PAs with the right tools to improve the transparency and accountability of their operations by supporting visual analysis of privacy issues considering both the technical and the social aspects at two different levels (e.g., design-time and run-time). On the other hand, VPP will equip citizens with the right tools to control the privacy of their data, through the development, monitoring, and enforcement of Privacy Level Agreements (PLAs). The VPP will consist of a series of software components (i.e., building blocks), which will be delivered by the VisiOn partners, by significantly advancing their existing software and tools, and integrate these components into the VPP.

[1]http://www.visioneuproject.eu/

The VPP will be tested and validated by two different types of pilots that involve two different types of PAs (municipalities and health care departments) and using various stakeholders (i.e., public administration, citizens, and third parties), where the first type will represent scenarios to demonstrate situations where citizens share their data with a PA. While the last type will represent scenarios where PAs from two different countries (i.e. cross-border scenarios) must exchange patient data to provide some required healthcare. To this end, one main objective of VisiOn project is capturing the VPP users requirements, which will be used as a basis to define the main functionalities and qualities required by its two types of users. In addition, such requirements will be used by component developers to identify how their tools need to be extended and integrated into the VPP.

III. A Privacy Engineering Process

The process for eliciting, classifying, prioritizing and validating the VisiOn user requirements (depicted in Figure 1) consists of four main interrelated activities. In what follows, we describe each of these activities:

1. Stakeholder analysis aims for better understanding the overall scope of the VisiOn platform by identifying all the stakeholders that may influence, or may be influenced, by the platform, as well as classifying them into coherent groups in order to better identify their needs and expectations concerning the platform. Therefore, we depend on the VisiOn proposal and the available documentation that has been obtained from the partners[2] as input to analyze the stakeholders, from which we identify three main stakeholders' roles: PA, citizen and component provider along with their main expectations concerning the platform. This activity produces the *stakeholders' description*, which is used by the requirements elicitation activity and is a critical factor for its success, and thus *stakeholders' analysis* is the first activity to be executed.

2. Eliciting the VisiOn user requirements. Aims to discover, acquire, and elaborate the requirements of the VisiOn platform through its main stakeholders, users, available documentation, etc. Among existing elicitation techniques (e.g., interviews, questionnaires, task analysis, scenarios, prototyping, etc.), we adopted two different techniques to elicit the requirements: (1) *questionnaire-based technique* since it has several characteristics that fit our needs, such as collecting multiple stakeholders' requirements simultaneously, being low-cost technique, eliciting the actual user requirements, and most importantly the flexibility in contacting the stakeholders/users. In the context of VisiOn, such flexibility is required since we rely on the VisiOn partners to provide us both their own perspective (PA) and their users/clients' perspective (citizen), and (2) *scenario-based technique* since such technique enables for interactively involving the partners during the requirements elicitation process, and enables for eliciting more specific requirements.

[2]Partners refer to the full consortium of the VisiOn project

This activity is composed of three main sub-activities: *2.1 Questionnaire-based requirements elicitation*, *2.2 Scenario-based requirements elicitation*, and *2.3 Eliciting the VisiOn user requirements from questionnaires and scenarios* that elicit the requirements from the two different techniques, and then integrate them together, which improves the quality of the elicited requirements. Note that this activity is repeated twice, with the main purpose of eliciting more detailed VisiOn users requirements in the second iteration. In what follows, we describe each of these activities:

2.1 Questionnaire-based requirements elicitation. This activity is composed of two main activities *2.1.1 Design the questionnaire I/II* and *2.1.2 Filling the Questionnaire I/II*, where the first aims to design the questionnaire template, and the last aims to share the questionnaires with the stakeholders and receive their feedback (see Figure 1). In the first iteration, the first questionnaire is designed and filled by the stakeholder, while in the second iteration the second questionnaire is designed and filled.

2.2 Scenario-based requirements elicitation. We asked the VisiOn partners to define several scenarios where the management of personal information is critical for both citizens and PAs, and then we asked them to model these scenarios with requirements modeling language, namely STS-ml [15], where each of the produced models was used to elicit VisiOn user requirements. Similar to activity 2.1, activity 2.2 is repeated twice, where scenarios I and scenarios II are modeled in the first and second iteration of the activity respectively.

2.3 Eliciting the VisiOn user requirements from questionnaire I/II and scenario I/II this activity is repeated twice in the process and in each occurrence. It takes both the filled questionnaires that resulted from activity (2.1) and the modeled scenarios produced by activity (2.2) as an input; where each questionnaire and scenario is carefully checked and used to elicit the VisiOn user requirements.

3. Classifying, prioritizing and validating the VisiOn user requirements. Aims to collect feedback from all stakeholders in order to classify, prioritize and validate the requirements we collected so far, which enables producing a classified, prioritized and validated set of VisiOn user requirements. Moreover, the requirements classification allows producing the VisiOn requirements taxonomy, which enables the different partners to better understand and deal with the requirements. This activity was performed by designing a questionnaire and organizing several individual meetings with the VisiOn partners to collect their feedback.

4. Consolidating the VisiOn user requirements. It is the fourth and final activity in the process, and it aims to verify the final list of VisiOn user requirements with VisiOn partners. Specifically, we performed five different checks (validity, completeness, consistency, realism and verifiability) to verify that the requirements capture all the functionalities and qualities required by the users (PAs and citizen), to verify that the requirements are consistent with one another, and to verify with component developers that the requirements can actually be implemented.

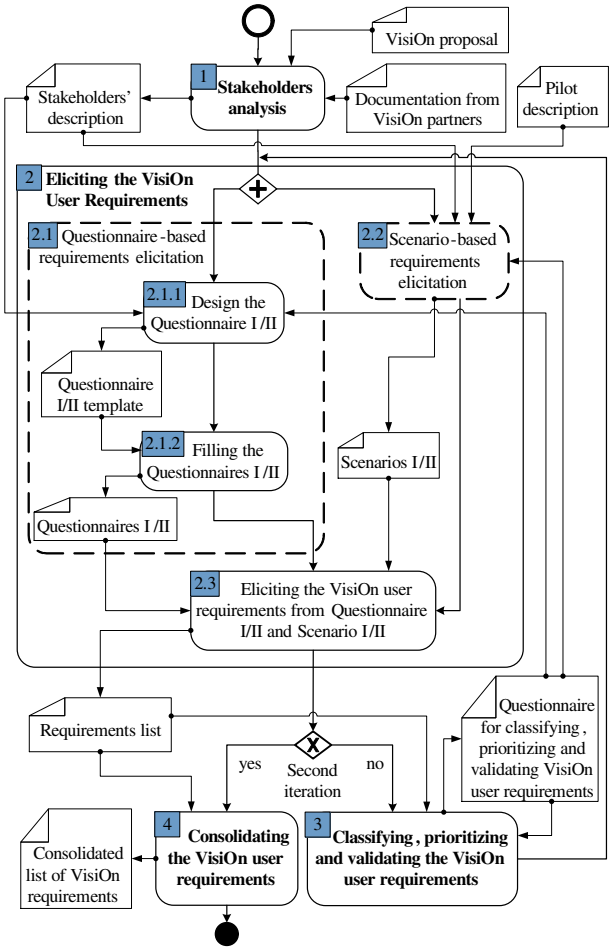

Fig. 1. The process for the elicitation, classification, prioritization, and validation of VisiOn user requirements

IV. Analyzing the VisiOn Privacy Platform Requirements

This section gives a detailed description of how the process has been used to analyze the VisiOn users requirements.

A. Stakeholder Analysis

This section summarizes our activities of classifying and analyzing the stakeholders of the VisiOn platform.

1) Stakeholder Classification: Depending on the available resources (VisiOn project proposal, partners documentation, etc.), we have identified three main types of VPP stakeholders, namely: *(1) Citizen*, an entity that will use VisiOn to define, visualize and control how its personal information is used by the others (e.g., PAs); *(2) PA*, an entity that will use VisiOn to visualize, manage and control how the citizens' personal information is used and for which reasons by its own services and services provided by others[3]; and *(3) Component provider*, representing a VisiOn partner that provides technical

[3]Citizens and PAs roles can be generalized to a User stakeholder role

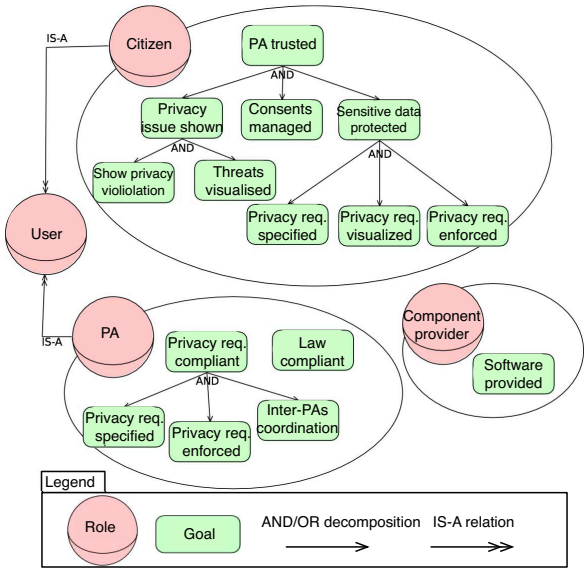

Fig. 2. Objectives of stakeholders of VisiOn

components for the architecture of the VPP. They contributed with requirements of each component and information of the integration among the components of the VPP.

2) Stakeholders Objectives: After identifying the three main types of VPP stakeholders, we analyzed each of them in terms of its main objectives from the VisiOn project proposal. Figure 2, shows the main stakeholder types along with their objectives represented with STS-ml [15]. In STS-ml, the stakeholders are specified with the help of the concept of *role*, which is graphically represented with a pink solid circle, while goals, an objective a stakeholder aims to achieve, are graphically represented as green solid ovals. The oval shapes attached to stakeholders represent their *scopes*: the set of goals the stakeholder wants or is in charge for fulfilling, as well as how it fulfills them. That is, if a goal is placed inside a role's scope then the goal is considered as assigned to the stakeholder connected to scope. For example, in Figure 1 *Citizen* is in charge of the goal *PA trusted*. Goals can be refined through "and-decomposed" or "or-decomposed" into subgoals, where in and-decomposition all subgoals must be achieved to fulfill the main goal, while only one of the subgoals must be achieved to fulfill the main goal in the or-decomposition.

B. Eliciting the VisiOn User Requirements (first iteration)

This section describes our activities for eliciting the VisiOn user requirements during the first iteration of this activity.

1) VisiOn Requirements Questionnaire I: In what follows, we describe how the first VisiOn requirements questionnaire was designed and filled by the partners.

VisiOn Questionnaire I (Q1) Design. The requirements for a system can be elicited from several sources [16], including stakeholders, users, documentation, other existing systems [17]. Therefore, the first VisiOn Questionnaire (Q1) template was designed to elicit requirements from the following three main sources: *(1) application domains:* the application domain should be explored together with its political, organizational, social aspects, the domain constraints that may influence the system [17], [18]; *(2) stakeholders:* are the entities who can influence, or are being influenced by the system, where identifying and analyzing the stakeholders is essential for the success of the requirements elicitation process [14]; and *(3) intended users:* are the entities who directly interact with the system to perform their work, and they play a central role in the requirements elicitation process as some requirements can be defined only by them (e.g., usability, supportability) [19].

To this end, the questionnaire contains four main sections to be filled by the partners concerning: *(1) application domains*, *(2) stakeholders*[4], *(3) intended users*, and *(4) examples of usage* that identify at least three possible scenarios in the application domains where users use VisiOn platform.

VisiOn Questionnaire I (Q1) - Filling and Refining. We shared Q1 template with four End-User (E-U) partners that represent both PAs and citizens, and we asked them to fill and return. The partners started to contact us few days after sending the questionnaire, asking for some clarifications about some general concerns related to their input, and they asked for more details about some particular questions. We analyzed the returned questionnaires, and we added our comments wherever we needed a clarification or more descriptions from the partner. In several cases, we supported our comments with general examples to assist the partner in replying to them. And then, we sent back the questionnaire to the partners to refine it and to send it back to us again. In some cases, the questionnaire was sent back and forth to the partner several times until their input is clear and understandable. In summary, 24 stakeholders, 8 stakeholders (not users), and 12 users of VPP along with their objectives, excepted functionalities and qualities were identified.

2) Modeling and Analyzing the Scenarios I: We asked the VisiOn partners to define three scenarios where the management of personal information is critical for both Citizens and PAs. Moreover, we asked them to use STS-ml [15] for modeling these scenarios. STS-ml requirements models are created by the construction of three complementary views:

(i) The social view (shown in Figure 3) is built on three concepts: *actor* that can be divided into a *role* (e.g., *Citizen*) or an *agent* (e.g., *Management system*), *goal* (e.g., "Birth certificate obtained") and *document* that is tangible supporting materials used to contain data (e.g., "Birth certificate"). A goal may *produce* a document, i.e., the document is created when the goal is achieved (e.g., "Birth certificate issued" will *produces* the document "Birth certificate"), and it may *read* a document, i.e., the goal need to read the document in order to be achieved (e.g., the goal "Birth certificate obtained" need to read the "Birth certificate"). The interactions between

[4]To extend our knowledge about the stakeholders analysis (activity 1), and uncover any stakeholder that has not been identified yet

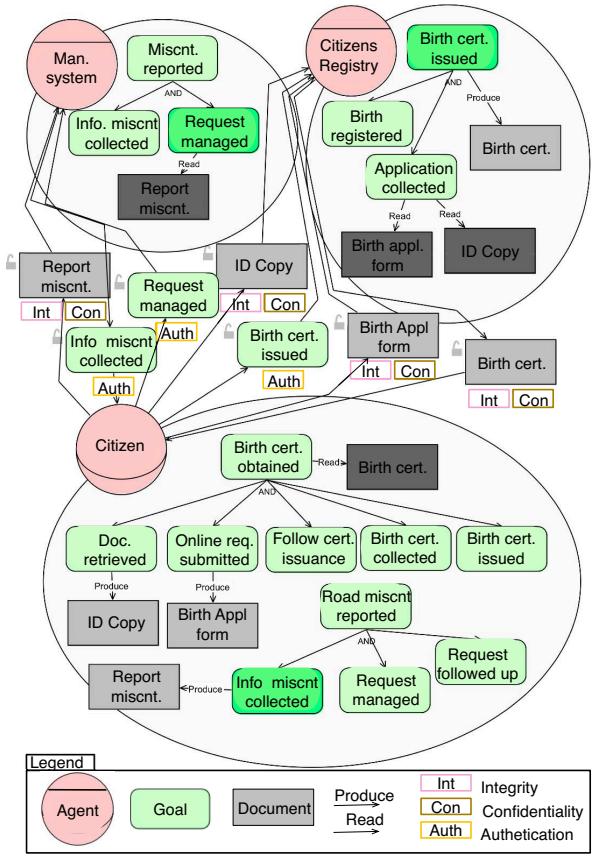

Fig. 3. STS-ml social view

actors are represented with two relations, *transmission* and *delegation*. The former represents the *transmission* of a document between two actors, while the latter represents the *delegation* of a goal, i.e., the assignment of an objective from an actor to another actor. For example, in Figure 3 *Citizen transmits* the "ID copy" to *Citizen Registry*, and it *delegates* the goal of "Birth certificate issued" to the same agent. On Each *transmission* and *delegation* security requirements can be specified, in Figure 3 three of them are shown: *integrity* means that the document received is the same as the document sent, *confidentiality* means only authorized users can read the document that is sent. While, if a *delegation* is marked with *authentication*, the source and destination actors must prove their identity, e.g., using an authentication mechanism.

(ii) The information view is built on two concepts: *document* and *information*. The latter represents intangible data that is stored in a document. Moreover, the relation *Tangible By* specifies that information is stored in that document. While the *Own* relation specifies that an actor is the legitimate owner of information. For example, in Figure 4 the *Citizen* role *own* information "Name" that is stored in "Birth certificate".

(iii) The authorization view represents the authorizations

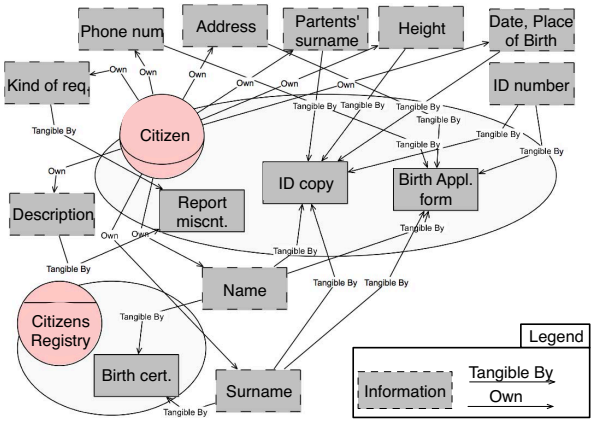

Fig. 4. STS-ml information view

that actors grant to one another over their information. Figure 5 shows the authorization relation that consists of three parts: (i) a set of authorizations, i.e., **R**ead, **M**odify, **P**roduce and **T**ransmit that are specified in the upper part; (ii) a set of information, i.e., the target of the authorizations; and (iii) a set of goals, i.e., the scope of the authorization. For example, the authorization relation between *Citizen* and *Management system* authorizes the latter to read and transmit "Picture", "Description", "Location details" and "Kind of request" information, without any restriction on the scope, since the scope part is empty.

In particular, each partner was assisted by a modeling expert while modeling its scenarios. The models have been refined iteratively through several modeling sessions until they capture all the information that the partner wants to include in the model. The resulting models were analyzed by STS-ml tool to detect any modeling deficiencies, and when they were verified correct, they were used to elicit VisiOn user requirements.

3) Eliciting the VisiOn user requirements from questionnaires I and scenarios I: After the questionnaires are filled and refined, and the scenarios are modeled and analyzed, we used both of them to elicit 91 stakeholders' needs[5], which we used to elaborate the first set of the VisiOn user requirements

[5]We identify the stakeholders' needs for requirements traceability reasons

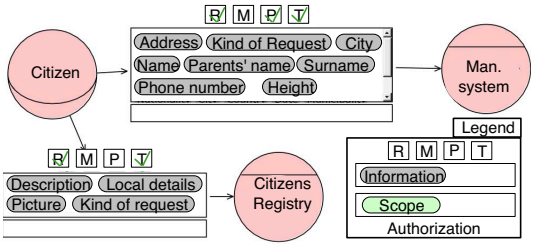

Fig. 5. STS-ml authorization view

(99 requirements). More specifically, when the stakeholder's need is clear enough it is considered as a requirement. While when the need is not clear, it is refined into a requirement or more. Finally, we have shared the VisiOn user requirements with the partners to receive their feedback, which we took into account while revising the requirements list.

C. Classifying, Prioritizing and Validating the VisiOn User Requirements

This section describes the questionnaires and meetings, we performed during the Technical Meeting[6] to classify, prioritize and validate the requirements.

1) VisiOn User Requirements Classification, Prioritization and Validation Questionnaire - Design: The questionnaire presents a table that contains the requirements elicited from both Q1 and scenarios, where each requirement has been assigned a *type* based on our proposed classification, a *priority* of the requirement to be filled by the partner (1 low - 5 high), and a text box to add any *comment/suggestion* concerning the requirement. In particular, 17 individuals from nine different partners have participated in this activity, and we asked them to analyze the table, to provide priorities and comments for each requirement and, possibly, to extend the list with other relevant requirements and/or new classifications. Moreover, we provided them with a table that contains a *mapping* between the requirements and the VisiOn component that will realize them, and we asked them to provide feedback.

2) VisiOn User Requirements Classification: Requirements classification is the activity that takes the unstructured collection of requirements and groups the related requirements into coherent clusters [20]. Requirements can be classified in many ways [21], yet it is generally accepted in the RE community that requirements can be broadly classified under functional and non-functional requirements, where the first type refers to the functionalities that the system shall deliver, and the last refers to how the system shall deliver such functionalities [20], [22]. Other types of requirements that can be used to sub-classify requirements have been proposed in the literature such as security [9], trust [8], information quality [23], etc.

To this end, we proposed a classification of the VisiOn requirements that is based on well adopted taxonomies from the literature (e.g., [8], [9], [24]–[28]). We sub-classify privacy requirements based on the common aspects of privacy identified from on the feedback we received from the stakeholders taking into consideration the five components of VisiOn Platform (privacy assessment, privacy requirements, privacy specification, privacy run-time, and privacy visualization component). Then we provide the partners with a table that contains the list of requirements that has been assigned a type based on our proposed classification, and we asked them to provide feedback. The returned feedback was carefully examined while producing the final taxonomy of the VisiOn requirements (depicted in Figure 6):

[6]Occurred in Rome during 14-15th of October with the participation of all VisiOn partners

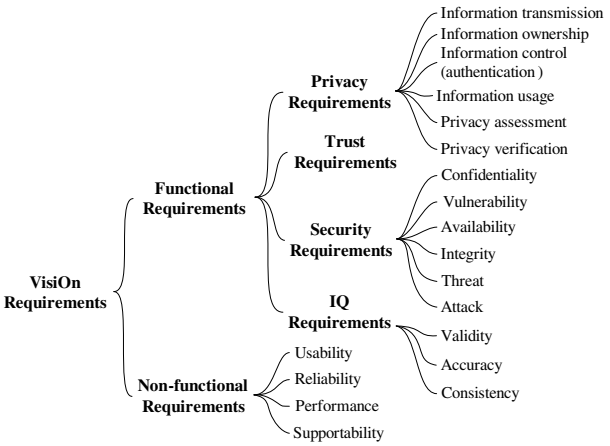

Fig. 6. VisiOn user requirements taxonomy

- Non-functional requirements are classified under four main categories [25]: 1- usability, 2- reliability, 3- performance, and 4- supportability.
- Functional requirements have four main categories:
  1) Trust requirements [8], [9].
  2) IQ requirements have three main sub-categories [27], [29]: 1- accuracy, 2-validity, and 3- consistency.
  3) Security requirements have six main sub-categories [26], [28]: 1- confidentiality, 2- integrity, 3- availability, 4- vulnerability, 5- threat, and 6- attack.
  4) Privacy requirements have six main sub-categories: 1- information ownership, 2- information control (authentication), 3- information usage, 4- information transmission, 5- privacy assessment, and 6- privacy verification.

3) VisiOn User Requirements Prioritization: Requirements prioritization is the process of classifying the requirements based on their importance [20], [30], which enables system developers to make decisions on which requirements should be implemented. Among the several requirements prioritizing techniques that have been proposed (e.g., Analytic Hierarchy Process (AHP), Cumulative Voting, Ranking, Ten Requirements, etc), we have adopted the Numerical Assignment (Grouping) [31], in which requirements are classified into different priority groups. A main reason for adopting this technique is its simplicity, and it is standardized (see IEEE Std. 830-1998 [32]). Specifically, we asked the partners to prioritize each of the requirements on an ordinal scale from 1-5, where 1 is the least important and 5 is the most important. After that, we classified the partners based on their role in the VisiOn project under End-Users (E-U) (i.e., Citizens and/or PAs), System Integrators (SID) and Research and Academic (R-C). Then we calculated the requirements priority value for each of three partners' types. This was followed by assigning qualitative values instead of the numbered ones to enable qualitative reasoning concerning requirements prioritization.

In particular, priority is **H**igh if its priority is at least four, it is **M**edium if its priority is at least three and less than four, and the priority is **L**ow if it is less than three. Furthermore, following [33], we assigned different weights to the input received from the different partners categories. We considered the E-U partners input as the most relevant since they represent the actual users of VPP (Citizens and PAs), followed by the SID partners input since they have experience in developing and commercializing software products, while the least important is the R-C partners input since they have experience in developing software products.

Table I shows how we determine the priority of the requirements based on the input from the different partners. The priority values are evaluated qualitatively as follows: we have priority **H** when the priority expressed by E-U is **H**, while both of the priority values expressed by SID and R-C are at least **M**. The priority value is **M** if it was expressed by E-U as **M**, and both of the priority values expressed by SID and R-C are at least **M**. Finally, the priority is **L** if the priority expressed by E-U is **L** regardless of the input provided by SID and R-C, or when the priority expressed by E-U is **M**, and at least one of the SID and R-C has expressed it **L**.

4) VisiOn user requirements validation: The first elicited set of VisiOn user requirements was validated by the feedback received from the partners and the individual meetings we arrange with them during the Technical Meeting.

D. Eliciting the VisiOn User Requirements (second iteration)

This section describes our activities for eliciting the VisiOn user requirements during the second iteration of this activity.

1) VisiOn Requirements Questionnaire II: In what follows, we describe how the second VisiOn requirements questionnaire II was designed and filled.

VisiOn Questionnaire II (Q2) - Design. The main aim of Q2 was eliciting detailed requirements from the two types of VisiOn users (PA and citizen) concerning their functionalites and qualities, how they are expected to interact with VisiOn to perform such functionalities, and how the platform is expected to realize their defined qualities. In addition, Q2 was designed in a way to link the users' feedback with the different components of the VPP, which enable the component developers to better understand how they can modify and extend their tools/components to meet the defined functionalities and qualities. Therefore, we provided a specialized version of the questionnaire for each partner taking into consideration his/her input in Q1. In particular, Q2 was designed to include two sub-questionnaires specialized for the two types of VisiOn users (PA and citizen), to be filled by the partner for each PA and citizen users identified by them in Q1. In what follows, we describe each of the sub-questionnaire:

Each of these sub-questionnaire contains six sections. The first section is different between the two sub-questionnaires, while in the *PA user questionnaire* it aims to describe the *(1) system analysis:* that captures the interaction between the VPP and the system(s) that is/are using the citizens' information, and in the *citizen user questionnaire* it aims

TABLE I
PRIORITY MATRIX

Priority	H	M	M	M	L	L	L
E-U	H	M	H	H	L	M	M
SID	M	M	L	-	-	L	-
R-C	M	M	-	L	-	-	L

to describe the *(1) privacy requirements identification:* that captures how the citizen is expected to interact with the VPP to specify its privacy requirements and how the VPP is expected to assist him/her during the process, etc. While the two questionnaires share the same following five sections, *(2) privacy requirements visualization:* to capture what kind of information a PA/citizen might need to visualize, how it needs to visualize it, etc.; *(3) privacy requirements analysis:* to capture what kind of analysis the VPP should provide, what is the expected output of such analysis, etc.; *(4) privacy requirements analysis at run-time:* to capture what kind of analysis the VPP should perform at run-time, what is the expected output for such analysis, etc.; *(5) Privacy Level Agreement (PLA):* to capture the PA/citizen expectations about the PLA, which enable us to extend our knowledge concerning the PA/citizen objectives; and *(6) examples of usage:* to elicit requirements of the PA/citizen that the partner might forget to mention while compiling the previous sections.

VisiOn Questionnaire II (Q2) - Filling and Refining. In line with what we did for Q1, we shared Q2 with three E-U partners and we asked them to fill and return. Similar to the Q1 filling and refining process, we assist them during this process. After receiving the filled questionnaires, we analyzed them, and we contacted some partners to refine their input until it is clear. In summary, very detailed needs of six PAs and three Citizens concerning the VPP were identified.

2) Modeling and Analyzing the Scenarios II: Similar to what we did in the first iteration of this activity, we asked the VisiOn partners to extend the STS-ml models of the scenarios they created earlier. This led to the creation of more complete models that cover, with great details, the scenarios. Therefore, they can be used to better identify the related VisiOn user requirements on the part of the system included in the scenarios.

3) Eliciting the VisiOn user requirements from questionnaires II and scenarios II: Similar to the first iteration of this activity, we used both of the questionnaires and scenarios to elicit the second set of VisiOn user requirements, which have been used to refine and extend the already elicited requirements to produce the final list of VisiOn user requirements (41 new requirements).

4) Consolidating[7] the VisiOn User Requirements: Requirements validation is concerned with showing that the set of requirements is correct, complete, consistent among one another, and they actually define the system that the stakeholders expect [20], [34]. Requirements validation is very important

[7]Requirements consolidation is used to refer to the validation of the final list of VisiOn user requirements

activity, since detecting errors in the requirements during the design phase is much less expensive and time-consuming than discovering such errors after the system implementation [9]. Sommerville [20] suggests five checks (validity, completeness, consistency, realism, and verifiability) to be performed on the requirements to validate them. In what follows, we discuss how we performed each of these checks to reach the final consolidated list of VisiOn user requirements:

1) *VisiOn requirements validity check* aims to verify the elaborated requirements with all the stakeholders of the system-to-be. We performed this check by sharing the VisiOn user requirements with all the partners, and we asked them to carefully check them and provide us with their feedback. The feedback contains suggestions to refine some requirements to better define the functionalities/features they require the system to deliver.
2) *VisiOn requirements completeness check* aims to verify that the elaborated requirements capture all the functions, features, constraints, etc. expected by the system users. We performed the completeness check by asking the End-User (E-U) partners that represent both PAs and citizens to check the elaborated list of requirements and whether they describe all the functionalities and features they expect the system to deliver. Some partners asked to add new requirements to the list that were not included in the requirements we elaborate.
3) *VisiOn requirements consistency check* aims to verify that the elaborated requirements are consistent with one another, i.e., no inconsistency should exist among the requirements. The consistency check was able to detect some conflicts among the requirements. However, we manage to solve this issue by revising the conflicting requirements with the help of the partner(s) who identify such requirements[8].
4) *VisiOn requirements realism check* aims to verify that the requirements can actually be implemented. We performed this check by sharing the requirements list with the partners that are responsible for developing the components of the VPP, and we ask them to carefully check the requirements list and provide us with their feedback. The feedback contains suggestions to revise several requirements, and mark 15 of them as out of the VPP scope. In addition, we have a long Telco meeting with them to discuss the requirements one-by-one. After the meeting, the requirements list was revised accordingly. A snapshot of the shared requirements table is shown in Figure 7.
5) *VisiOn requirements verifiability check* requirements should be written in a clear and understandable way so that they are verifiable by the different stakeholders, which reduce any potential dispute between the stakeholders. This check was done by sharing the final list of requirements with End-Users (PAs and Citizens) and Component developers, i.e., both of them were able to check and provide their feedback concerning the same requirements list. Moreover, we kept records of all the documents we shared with the different partners along with their feedback on these documents, which enables for resolving any potential dispute between the two sides.

[8]We depend on STS-ml to analyze the consistency of some of the functional requirements (e.g., security, trust, etc.)

ID	Requirement Description	Type	Source	Req. of PA/C	Component	Priority
1	The VisiOn platform shall provide user-friendly interfaces for its users.	NFR/ Usability	[OPBG_ST #2-1-R1]	PA-C	PA, PV	H
2	The VisiOn platform shall support access to the citizen's information to authorized users only.	SR/Confidentiality	[OPBG_AD#2-10-R1]	PA-C	PR, PS	H
3	The VisiOn platform shall analyse the users' authorizations based on their needs to perform their activities.	PR/Info ownership	[OPBG_AD#2-10-R1]	PA-C	PR, PS	H
Added	The VisiOn platform shall control the usage of its services to authorised users' only.	PR/Info ownership	[OPBG_AD#2-10-R1]	PA-C	PA, PV	H

Fig. 7. A Snapshot of the requirements table shared with the partners

A snapshot of the table that contains the consolidated VisiOn user requirements is shown in Figure 8, where each requirement is described with the following attributes:

- *Req. ID:* A unique identifier for each requirement.
- *Description:* a textual description of the requirement, and a clarificatory text for some requirement.
- *Type:* the type of the requirement based on our taxonomy.
- *Source:* used for traceability reasons, requirement source is represented with a unique identifier that specifies the source where the requirement has been elicited from.
- *Req. of (PA/C):* whether it is a requirement for Public Administration (PA) and/or for Citizen (C).
- *Component:* it identifies the component(s) that will realize such requirement.
- *Priority (H/M/L):* indicates how important the requirement is in order to achieve the objectives of the project: 1- (H)igh: Must have, 2- (M)edium: Should have, and 3- (L)ow: Nice to have.

V. Findings and Lessons Learned

Through using our process for eliciting, classifying, prioritizing and validating the VisiOn user requirements, we have faced several challenges related to the different activities we performed. In what follows, we summarize our findings and lessons learned.

Classify the stakeholders into coherent groups: stakeholders involvement in RE activities is related to their types, which can be used to classify them into coherent groups to better communicate with them to understand their requirements (e.g., requirements elicitation activity), integrate them into the different RE activities (e.g., requirements consolidation activity), and weighted their feedback based on their types (e.g., requirements prioritizing activity).

Consider questionnaire-based requirements elicitation: questionnaire-based technique can be used to collect multiple stakeholders' requirements simultaneously, it is low-cost technique, and it can be used to elicit the actual user requirements,

ID	Requirement Description	Type	Source	Req of PA/C	Component	Priority
1	The VisiOn platform shall provide user-friendly interfaces for its users.	NFR/ Usability	[OPBG_ST#2-1-R1]	PA-C	PA, PV	H
2	The VisiOn platform shall support access to the citizen's information to authorized users only.	SR/ Confidentiality	[OPBG_AD#2-10-R1]	PA-C	PR, PS	H
3	The VisiOn platform shall analyse the users' authorizations based on their needs to perform their activities.	PR/ Info ownership	[OPBG_AD#2-10-R1]	PA-C	PR, PS	H
4	The VisiOn platform shall control the usage of its services to authorised users' only.	PR/ Info ownership	[OPBG_AD#2-10-R1]	PA-C	PA, PV	H

Fig. 8. A Snapshot of the consolidated VisiOn user requirements

if the questionnaire was well designed. A main limitation of questionnaires is that they provide no mechanism for the participants to request clarification or correct misunderstandings. However, we overcame this limitation by providing answers, feedback and the required support for all the participants during the requirements elicitation process.

Consider two techniques for requirements elicitation: adopting two different techniques for requirements elicitation, significantly improved the quality of the requirements we elicited. For example, the same requirement might be elicited by the two techniques, yet it is unlikely that both techniques elicit the exact same requirement. Thus, the two versions of the requirement can be used to produce more detailed requirement. Moreover, it is recommended that the elicitation techniques are performed by two separate teams, which reduces the impact that one technique might have on the other, and in turn might influence the quality of the elicited requirements.

Propose a taxonomy of requirements: proposing an agreed upon taxonomy of the requirements enables the stakeholders to better understand the requirements by reducing or removing any vagueness while dealing with them, which contributes to better understanding how requirements can be realized. Moreover, such taxonomy can help in defining the system architecture in terms of its main components, which facilitates the mapping between the requirements and the components that will be used to realize them. For example, one main problem we faced is dealing with privacy requirements, since most existing works do not provide any agreed upon method for classifying such requirements. However, we solved this problem in the requirements taxonomy we proposed, in which privacy requirements have been analyzed in terms of six sub-dimensions that we have defined based on the main aspects of privacy we identified based on the stakeholders' feedback taking into consideration the five components of VPP.

Map requirements to system components: nowadays, many systems are developed by modifying existing components of systems, and these components might be developed by different developers. In this context, a developer might not know that the component(s) it is responsible for developing, is supposed to realize a specific requirement. Therefore, each requirement should be mapped to the component(s) that will realize it, which enable the component developers to understand better their responsibilities, and how they should extend their component(s) to realize such requirements. In addition, it facilitates performing the *requirements realism check*.

Consider requirements dependency along with requirements prioritization: despite the fact that the RE community agrees on the importance of requirements dependency [31], [35], it is largely neglected in requirements prioritization process [35]. To this end, we presented a table that captures three different relations among requirements (requires, increases/decreases the value of), which enables for better decisions concerning the requirements implementation. For example, a requirement might be classified as low priority (might not be implemented) based on the feedback of the stakeholders, yet it might be *required/increases the value of* a high priority requirement(s) (should be implemented).

Maintain requirements traceability: the VisiOn requirements have resulted from an iterative process, where each requirement might be elicited from more than one source, and it might be rephrased several times as well. Therefore, in order to know where the requirement has been first identified, and what kind of modifications have been applied to it. We have assigned each requirement with a unique identifier that can be used to easily trace it back to its original source.

Guarantee the requirements completeness: End-Users might not be able to define all the functionalities/features that VPP should deliver. Thus, to guarantee that the requirements are complete for developing the VPP, we compared between the functionalities/features of VPP derived from the end-users requirements and the VisiOn functionalities/features identified in the VisiOn proposal. We identified seven VPP proposed functionalities/features that were not captured by the requirements of the End-Users. Therefore, we discussed this issue with the component providers[9], and we decide to include these functionalities/features as new requirements for VPP.

Define a glossary of terms: the VisiOn project consortium is composed of several partners with different backgrounds. Therefore, it was not easy during the early stage of the requirements elicitation process to have a common understanding of the feedback we receive from the partners. For example, the term "system" was interpreted by Research and Academic (R-C) partners as the target system that uses the citizens' information, while it was used by End-Users to refer to VPP. We solved this issue by proposing a VisiOn glossary of terms that have been shared and agreed upon by all partners.

Document all related information: during the early stages of the requirements elicitation process, we faced several disagreements about how we interpret the partners' feedback. In order to avoid similar situations with the partners concerning their feedback, we start to document their participation in all the activities we performed (e.g., questionnaires, scenarios, meeting, Teleco meeting[10], etc.).

[9]Stakeholders of VPP, i.e., they can be a source for identifying requirements
[10]In case of Teleco meeting we document the meeting minutes

VI. Conclusions

In this paper, we have presented a Requirements Engineering (RE) process for eliciting, classifying, prioritizing and validating privacy requirements, the process is composed of several existing RE activities that have been adapted in order to deal with the privacy requirements for VPP. The process has been developed to be used for real world projects (e.g., industry). Therefore, we focused our effort to make the process easy to be used, and we accompanied each of its activities with a detailed description of how it can be performed. The process has been successfully used to elicit, classify, prioritize and validate the VisiOn user requirements, where these requirements have been used to define the main functionalities and qualities of two types of VPP users (e.g., PAs and citizens). In addition, the requirements have been used by component developers to identify how their tools need to be extended and integrated into the VPP.

Our process may suffer from the following limitations and threats to validity: *Hypothesis guessing* the participant's response might be influenced, when he/she knows, or guesses, the desired end-result. However, we tried our best to design the different questionnaires in a way that does not influence nor guide the participants. *Researcher expectations* that might be communicated unintentionally to the participants. To avoid such threat, we shared all the questionnaires with the partners who are not participants, and ask them to check whether the questionnaire is properly designed. Finally, the process has been applied to only one system (VPP), which threatens *the generalization of its findings*. However, we aim to better validate the applicability of the process by applying it to several case studies in different domains.

Acknowledgment

This research has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 653642 - VisiOn.

References

[1] A. Garg, J. Curtis, and H. Halper, "Quantifying the financial impact of it security breaches," *Information Management & Computer Security*, vol. 11, no. 2, pp. 74–83, 2003.

[2] U.S department of health and human services, "The HIPAA Privacy Rule," 2002. http://www.hhs.gov/hipaa/for-professionals/privacy/

[3] A. Acquisti, A. Friedman, and R. Telang, "Is there a cost to privacy breaches? an event study," *ICIS 2006 Proceedings*, p. 94, 2006.

[4] R. Gellman, "Privacy, consumers, and costs: How the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete," in *Digital Media Forum, Ford Foundation*, 2002.

[5] Z. Ebrahim and Z. Irani, "E-government adoption: architecture and barriers," *Business process management journal*, vol. 11, no. 5, pp. 589–611, 2005.

[6] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the pris method," *Requirements Engineering*, vol. 13, no. 3, pp. 241–255, 2008.

[7] A. Cavoukian, "Privacy by design: Origins, meaning, and prospects," *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards: Aspects and Standards*, p. 170, 2011.

[8] N. Zannone, "A requirements engineering methodology for trust, security, and privacy," Ph.D. dissertation, University of Trento, 2006.

[9] H. Mouratidis and P. Giorgini, "Secure Tropos: A security-oriented extension of the Tropos methodology," *International Journal of Software Engineering and Knowledge Engineering*, vol.17, pp.285–309, 2007.

[10] G. Wang, R. Valerdi, and J. Fortune, "Reuse in systems engineering," *Systems Journal, IEEE*, vol. 4, no. 3, pp. 376–384, 2010.

[11] T. D. Breaux and A. I. Antón, "Analyzing regulatory rules for privacy and security requirements," *Software Engineering, IEEE Transactions on*, vol. 34, no. 1, pp. 5–20, 2008.

[12] A. Martinez-Balleste, P. Perez-martinez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," *Communications Magazine, IEEE*, vol. 51, no. 6, pp. 136–141, 2013.

[13] S. Spiekermann and L. F. Cranor, "Engineering privacy," *Software Engineering, IEEE Transactions on*, vol. 35, no. 1, pp. 67–82, 2009.

[14] H. Belani, K. Pripuzic, and K. Kobas, "Implementing web-surveys for software requirements elicitation," in *8th International Conference on Telecommunications–ConTEL*, 2005, pp. 465–469.

[15] E. Paja, F. Dalpiaz, and P. Giorgini, "Modelling and reasoning about security requirements in socio-technical systems," *Data & Knowledge Engineering*, vol. 98, pp. 123–143, 2015.

[16] P. Loucopoulos and V. Karakostas, *System requirements engineering*. McGraw-Hill, Inc., 1995.

[17] D. Zowghi and C. Coulin, "Requirements elicitation: A survey of techniques, approaches, and tools," in *Engineering and managing software requirements*. Springer, 2005, pp. 19–46.

[18] M. Jackson, "The world and the machine," in *Software Engineering, ICSE 1995*. IEEE, 1995, pp. 283–283.

[19] B. Nuseibeh and S. Easterbrook, "Requirements engineering: a roadmap," in *Proceedings of the Conference on the Future of Software Engineering*. ACM, 2000, pp. 35–46.

[20] I. Sommerville, *Software engineering 8*. Pearson Education limited, 2007.

[21] A. Aurum and C. Wohlin, "Requirements engineering: setting the context," in *Engineering and managing software requirements*. Springer, 2005, pp. 1–15.

[22] L. Chung and J. do Prado Leite, "On non-functional requirements in software engineering," *Conceptual modeling: Foundations and applications*, pp. 363–379, 2009.

[23] M. Gharib and P. Giorgini, "Modeling and reasoning about information quality requirements," in *Requirements Engineering: Foundation for Software Quality*. Springer, 2015, pp. 49–64.

[24] D. J. Solove, "Conceptualizing privacy," *California Law Review*, pp. 1087–1155, 2002.

[25] J. Mylopoulos, L. Chung, and B. Nixon, "Representing and using nonfunctional requirements: A process-oriented approach," *IEEE Transactions on Software Engineering*, pp. 483–497, 1992.

[26] B. Standard, "Information security managementpart 1: Code of practice for information security management," *British Standard BS7799-1*, 1999.

[27] M. Bovee, R. P. Srivastava, and B. Mak, "A conceptual framework and belief-function approach to assessing overall information quality," *Journal of intelligent systems*, vol. 18, no. 1, pp. 51–74, 2003.

[28] N. Mayer, "Model-based management of information system security risk," Ph.D. dissertation, University of Namur, 2009.

[29] L. L. Pipino, Y. W. Lee, and R. Y. Wang, "Data quality assessment," *Communications of the ACM*, vol. 45, no. 4, pp. 211–218, 2002.

[30] M. Helfert and C. Herrmann, "Proactive data quality management for data warehouse systems." in *DMDW*, vol. 2002, 2002, pp. 97–106.

[31] P. Berander and A. Andrews, "Requirements prioritization," in *Engineering and managing software requirements*. Springer, 2005, pp. 69–94.

[32] I. C. S. S. E. S. Committee and I.-S. S. Board, "Ieee recommended practice for software requirements specifications." Institute of Electrical and Electronics Engineers, 1998.

[33] B. Regnell, M. Höst, J. N. och Dag, P. Beremark, and T. Hjelm, "An industrial case study on distributed prioritisation in market-driven requirements engineering for packaged software," *Requirements Engineering*, vol. 6, no. 1, pp. 51–62, 2001.

[34] A. Terry Bahill and S. Henderson, "Requirements development, verification, and validation exhibited in famous failures," *Systems Engineering*, vol. 8, no. 1, pp. 1–14, 2005.

[35] A. Herrmann and M. Daneva, "Requirements prioritization based on benefit and cost prediction: an agenda for future research," in *International Requirements Engineering, 2008. RE'08. 16th IEEE*. IEEE, 2008, pp. 125–134.