Enhancing Business Process Models with Trustworthiness Requirements

Nazila Gol Mohammadi and Maritta Heisel

paluno - The Ruhr Institute for Software Technology, University of Duisburg-Essen, Germany
{nazila.golmohammadi, maritta.heisel}@paluno.uni-due.de

Abstract. The trustworthiness of systems that support complex collaborative business processes is an emergent property. In order to address users' trust concerns, trustworthiness requirements of software systems must be elicited and satisfied. The aim of this paper is to address the gap that exists between end-users' trust concerns and the lack of implementation of proper trustworthiness requirements in software systems. We focus on the challenges of specifying trustworthiness requirements and integrating them into the software development process as business process models. This paper provides a conceptual model of our approach by extending Business Process Model and Notation (BPMN) for integrating trustworthiness requirements. Our proposed approach explicitly considers the trustworthiness of individual components as part of the business process models. We use an application example from the health care domain to demonstrate our approach.

Keywords: Trust, Trustworthiness, Requirements, Business Process Modeling.

1 Introduction

Advances on Information and Communication Technology (ICT) facilitate the automation of business processes and consequently increase organizations' efficiency. However, using new ICTs like cloud computing can also bring undesirable side effects, e.g., introducing new vulnerabilities and threats caused by collaboration and data exchange over the Internet. The consumers of business processes (either organizations or individuals) often hesitate in placing their trust in such technologies. Since trust is the prerequisite for performing many kinds of transactions and collaborations, users' concerns about the trustworthiness of these business processes, their involved apps, systems and platforms, slow down their adoption [6].

Business process models are frequently used in software development for understanding the behavior of the users, their requirements and for the assignment of requirements to particular well-defined business process elements. In business processes, resources are either human or non-human assets, e.g., software, apps or IT devices [3]. Non-human assets can provide either fully-automated or semi-automated support to the activity performers. Since people rely on these technical resources when performing their activities, trustworthiness properties of these technical resources play a major role in gaining the trust of end-users (e.g., the reliability of the system that deals with monitoring the vital signs of a patient). There are specific conditions that must be defined

concerning human resources that contribute as well to trustworthiness, e.g., people's skills and expertise when performing particular tasks. In addition to trustworthiness requirements on resource management, the usage of digital documents and data plays a central role in the trustworthiness. For instance, in order to respect privacy regulations, digital documents have to be protected from unauthorized use (e.g., being shared in public networks). This clearly demands the consideration of trustworthiness properties, and hence the specification of trustworthiness requirements on data objects by defining usage rules, as well as the respective mechanisms for enforcing the usage of such rules. Consequently, trustworthiness should be considered in the management of both human and non-human resources in all stages of the business process life-cycle: design, modeling, implementation, execution, monitoring and analysis.

In the state of the art, issues related to security have been widely studied. Since trustworthiness covers a broader spectrum of properties rather than just security, there is a gap in research when addressing socio-economical factors of trustworthiness [9]. Especially software systems that provide support to different stakeholders should fulfill a variety of qualities and properties for being trustworthy, depending on application and domain [10]. For instance, organizations require confidence about their business-critical data, whereas an elderly person using a health care service may be more concerned about reliability and usability.

In this paper, we aim at closing the existing gap between end-users' trust concerns and the lack of implementation of the appropriate trustworthiness properties in software systems. We focus on specifying trustworthiness requirements starting from the business processes level by providing modeling capabilities to understand and express trustworthiness requirements. Our approach specifies which functionalities with which qualities should be realized to address trustworthiness and gain the trust of the end-user. For instance, one of the factors for gaining trust is awareness. Business processes should include transparency capabilities either in the form of functionalities or qualities, e.g., defining notification activities or escalation events upon activities on users' sensitive data. Usability and quality of representation of this notification are quality-related aspects. We specify which kind of transactions and activities need to be transparent to which extent for which organization or users. We mainly conribute to 1) understanding trustworthiness requirements and integrating them into the business process model, and 2) delivering detailed documentation of trustworthiness requirements along with the business process models using Business Process Model and Notation (BPMN) [17].

Tools and services developers are supported through detailed trustworthiness requirements for the software and services to be built. Then, based on trustworthiness requirements embedded in business process models, they can make more informed design decisions. We also believe that once trustworthiness requirements have been considered and documented in business process models, they will not be ignored during design-time. To demonstrate the enhancement of business process models with trustworthiness requirements, we consider an example from the health care domain, namely, an Ambient Assisted Living (AAL) system.

The remainder of this paper is structured as follows: Section 2 provides a brief overview of the fundamental concepts and the background. Section 3 presents an overview of the state of the art. Section 4 describes the classification of trustworthiness require-

ments, which can be expressed in the business process model. Furthermore, it gives initial recommendations for modeling and documenting trustworthiness-related capabilities into the business process. Section 5 demonstrates our approach using an application example from AAL. Section 6 presents conclusions and future work.

2 Fundamental concepts and Background

This section introduces the notion of trust and moves on to define the meaning of trustworthiness. We then identify the relation between trust and trustworthiness. The basis of this work has been built up on the definition of trust and trustworthiness in our previous works in [10] and [9]. We distinguish between these two concepts.

Trust and Trustworthiness. *Trust* is defined as a "bet" about the future contingent actions of a system [22]. The components of this definition are belief and commitment. There is a belief that placing trust in a software or a system will lead to a good outcome. Then, the user commits the placing of trust by taking an action by using the business process and its software systems. This means, when a user decides to use a service, e.g., a health care service on the web, then he/she is confident that it will meet his/her expectations. Trust is subjective and different from user to user. For instance, organizations require confidence about their business-critical data, whereas an elderly person using a health care service (end-users) may be more concerned about usability. These concerns manifest themselves as trustworthiness requirements. Thus, business processes and their involved software systems and services need to be made trustworthy to mitigate the risks in engaging those systems and trust concerns of their users.

 Trustworthiness properties are qualities of the system that potentially influence trust in a positive way. The term *trustworthiness* is not used consistently in the literature. Trustworthiness has sometimes been used as a synonym for security and sometimes for dependability. However, security is not the only aspect of trustworthiness. Some approaches merely focus on single trustworthiness characteristics, e.g., security or privacy. Most existing approaches have assumed that one-dimensional properties of services lead to trustworthiness, and even to trust in it by users, such as a certification, the presence of certain technologies, or the use of certain methodologies. However, trustworthiness is rather a broad-spectrum term with notions including reliability, security, performance, and usability as parts of trustworthiness properties [15]. Trustworthiness is domain and application dependent. For instance, in health care applications, the set of properties which have primarily been considered consists of availability, confidentiality, integrity, maintainability, reliability and safety, but also performance and timeliness. Trustworthiness depends on a specific context and goals [10].

 For instance, in safety-critical domains the failure tolerance of a system might be prioritized higher than its usability. We, furthermore, need to consider different types of components, e.g., humans as social parts of the system or software assets as technical ones. Trustworthiness in general can be defined as the assurance that the system will perform as expected [10]. With a focus on business processes, we adopt the notion of trustworthiness from [10], which covers a variety of trustworthiness properties as contributing to trust. This allows us to consider trustworthiness as the degree to which relevant qualities (then referred to as trustworthiness properties) are satisfied.

Business Process Models. A business process model is the representation of the activities, documents, people and all the elements involved in a business process, as well as the execution constraints between them [4]. BPMN [17] is the standard for modeling business processes, which is extended and used widely in both, industry and research. Most important BPMN elements are as follows:

- Activities are depicted as rounded rectangular boxes.
- Events, which include receiving and triggering events, are depicted as circles.
- Data objects are depicted as a sheet of paper with the top right corner folded.
- Gateways, control of how the process flows, are depicted as diamonds.

An important feature of business process modeling is to create high-level, domain-specific models or abstractions rather than focus on platform-specific models which often involve details and dependencies of implementation and execution environments [12]. Business Process Management (BPM) is also considered to be a key driving force in building, maintaining, and evolving enterprise applications and an agile software development technology which transforms business strategies into IT executions in a fast and standardized way [2].

3   Related Work

The study of related work reveals some gaps in resource management in BPM with respect to trustworthiness. Several works have been performed to overcome the problem of resource assignment, some meta-models like [13], [25] and an expressive resource assignment language [3] have been developed. That language, RALPH [3], provides a graphical representation of the resource selection conditions and assignments. RALPH has a formal semantics, which makes it appropriate for automated resource analysis in business process models. Stepien et al. [20] present the user interfaces in which users can define the conditions themselves. The main gap is to address the broad spectrum of qualities which contribute to trustworthiness, and the necessity of defining conditions on resources and activities in business processes with respect to trustworthiness.

Plenty of works are done on security and to some extent on privacy. Short et al. [19] provide an approach for dealing with the inclusion of internal and/or external services in a business process that contains data handling policies. Wang et al. [26] developed a method to govern adaptive distributed business processes at run-time with an aspect-oriented programming approach. Policies can be specified for run-time governance, such as safety constraints and how the process should react if they are violated.

Resource patterns [18] are used to support expressing criteria in resource allocations. Business Activities is a Role-based access control (RBAC) [21] extension of Unified Modeling Language (UML) activity diagrams to define the separation of duties and binding of duties between the activities of a process. Wolter et al. [27] developed a model-driven business process security requirement specification which introduces security annotations into business process models for expressing security requirements for tasks.

However, the current state of the art in this field neglects to consider trustworthiness as criteria for the resources and business process management.

4   Modeling Trustworthiness Requirements in Business Processes Level using BPMN

Trustworthiness requirements are usually defined first on a technical level, rather than on a business process level. However, at the business process level, we are able to provide a comprehensive view on the participants, the assets/resources and their relationships regarding satisfaction of business goals, as well as trustworthiness goals. Integrating trustworthiness-related information into business processes will support designers and developers in making their design decisions. Trustworthiness requirements on the business process level can be translated into concrete trustworthy configurations for service-based systems. Therefore, our proposed approach can be applied on different abstraction levels. Figure 1 shows how trustworthiness requirements provided by our approach will streamline the software development. The left side of Figure 1 shows the level of abstraction for trustworthiness and their influences on different levels of abstraction on the system-side (simplified SOA layers). The refinement of trustworthiness requirements on different abstraction levels with a combination of goal models and business process models is presented in our other work [7].

The method for systematic identification and analysis of trustworthiness requirements is shown in Figure 2. Our proposed method uses goal and business process modeling, iteratively. Here, we only focus on enriching business process models with trustworthiness. The method starts with a context analysis. The major task of context analysis which we are interested in here is *"identification of end-user trust concerns"*. Prior to this step, the participants of a business and stakeholders are captured. We assume this information about the context is provided in a context model. This step is concerned with providing a list of trust concerns for the end-users. These trust concerns are captured by interviewing end-users, based on expertise of a requirements engineer. We provide a questionnaire to support the requirements engineer by identification of end-users' trust concerns [8]. Trust concerns and their dependencies on other participants in the business will be identified. Trust concerns are subjective and also domain and application dependent. The top-level business goals of identified stakeholders and business participants are captured in the goal models. We assume the goal models with the major intention of these involved parties/stakeholders are given. For satisfying the goals and
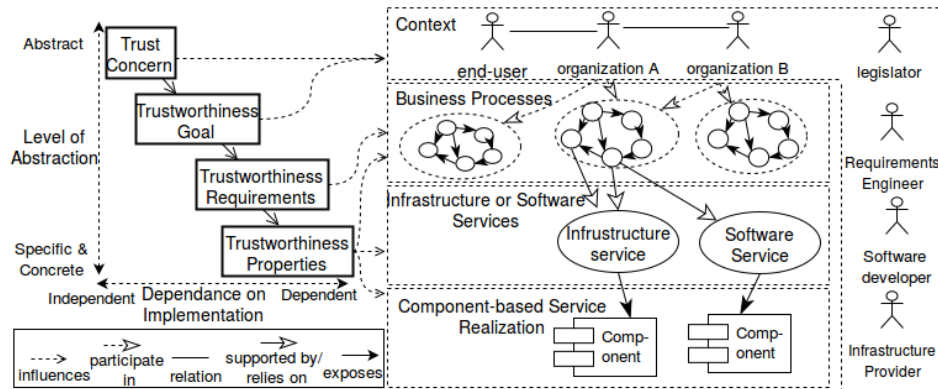

Fig. 1. Placing our proposed approach for enriching business processes with trustworthiness requirements and their alignment with software development
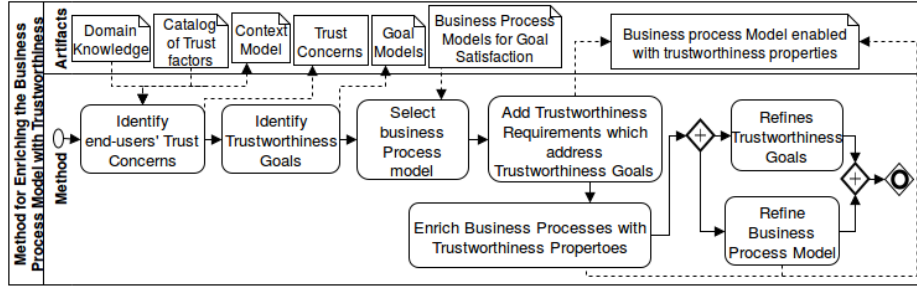
Fig. 2. Our method for enriching business processes with trustworthiness requirements

presenting how they are realized, the business process models are set up. To support this step, a catalogue of trustworthiness attributes which mitigate trust concerns is provided in our previous work in [9]. Next, based on trust concerns we *"identify the trustworthiness goals"*. The initial goal model will be refined and updated with trustworthiness goals and its relation to the other goals. We *select one of the business process models* for *including trustworthiness requirements satisfying trustworthiness goals*. This selection is based-on the location of the trustworthiness goal to the other goals. This steps goes through business process elements and control flow and questions whether a specific element in the business process is trustworthiness-related. Refinement of the business process model details business processes with including more concrete trustworthiness properties on resources, activities, etc. for satisfying trustworthiness requirements. This step can be concurrent to the goal and trustworthiness goal refinements, and both models can iteratively develop. Figure 2 gives an overview of the above mentioned steps and their input and output artifacts.

In this work, we focus only on specifying trustworthiness requirements in business process models. We propose a BPMN extension that allows the integration of trustworthiness requirements into a business process. We introduce trustworthiness elements for business process modeling which allows modeling and documenting trustworthiness requirements as well as placing a control to address the trust concerns of the end-users. Later, the resulting business process models with specified trustworthiness requirements can be used as basis for design and developing trustworthy software systems, applications, and even evaluation of the trustworthiness properties [6] e.g., privacy, reliability, confidentiality or integrity on an abstract level.

Business process modeling offers an appropriate abstraction level to describe trustworthiness requirements and later to evaluate trustworthiness-related risks. We describe an approach to first integrate trustworthiness requirements into a business process model. Then, we present a model-driven trustworthiness requirements refinement focusing on elements necessary for satisfying trustworthiness goals and also specifying constraints on elements of the business process (data objects, events, activities, resources etc.) to satisfy trustworthiness related qualities.

As stated in Section 3, there are BPMN extensions for the inclusion of different security requirements, e.g., non-repudiation, attack harm detection, integrity, and access control. There are also proposed languages for the formulation of security constraints embedded in BPMN. In all these approaches, only security requirements are incorporated into a BPMN process from the perspective of a business process analyst. In our

work, we consider a broad range of trustworthiness properties rather than just security. Furthermore, there is a rationale about where these trustworthiness requirements were originating from. Our proposed approach aligns organizational (business) requirements in an adequate way with trustworthiness requirements. Our approach tackles the problem of high-level and low-level trustworthiness requirements' misalignment between the business/organizational level and the application and software service level. This should satisfy business goals as well as trustworthiness goals of the end-users. The result allows a requirements engineer to create a business process specification that represents a process along with a set of trustworthiness properties that the generated software service, or app, needs to be compliant with. Therefore, this trustworthiness requirements specification allows the designer to make informed design decisions to put the right mechanisms into place.

4.1 Conceptual Model of the Enriching Business Process Model with Trustworthiness Requirements

We define the fundamental concepts and their relations in form of a conceptual model that is depicted in Figure 3. The conceptual model reflects the basic concepts of our approach.

The major concept of our method for eliciting and refining trustworthiness requirements is the combination of business process modeling using BPMN and goal models (cf. Figure 2). A trustworthiness goal is a special goal that addresses the trust concerns of users. The trustworthiness goal is satisfied by trustworthiness requirements, which can be realised by trustworthiness properties. In this paper, we focus on the part for analyzing and addressing the end-users' trust concerns, and expressing them in terms of either BPMN elements or the extended elements for trustworthiness. For instance, interactions points, defining trustworthiness-specific activities (e.g., notifications for satisfying transparency) or defining monitoring points where we can specify which part of the process needs to be monitored at run-time and what the desired behavior is. This will serve to derive trustworthiness requirements in the form of commitments reached among the participants for the achievement of their goals.

We use the term "business process element" to distinguish between generic types of BPMN, e.g., activity, resources like human resources or data objects and concrete
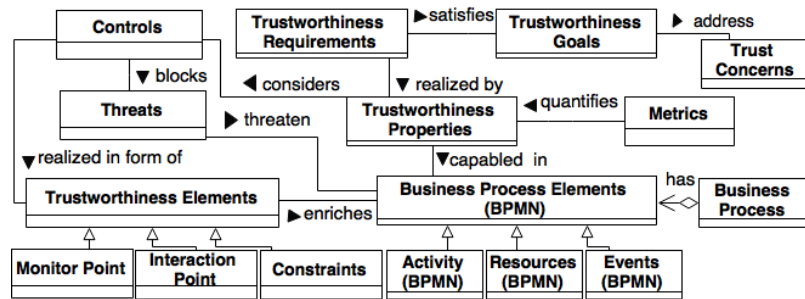

Fig. 3. The conceptual model for enriching the business process model with trustworthiness requirements

trustworthiness-related elements "trustworthiness element" (our extension) that can pertain to a type of BPMN elements, e.g., monitor point, interaction point and constraints.

A Threat is a situation or event that, if active at run-time, could undermine the value of trustworthiness by altering the behavior of involved resources or service in the process instance. Controls are trustworthiness requirements that aim at blocking threats. Metrics are used as functions to quantify trustworthiness. A Metric is a standard way for measuring and quantifying certain trustworthiness properties and more concrete quality properties of an element [10], [5].
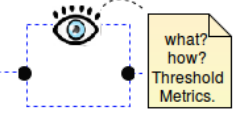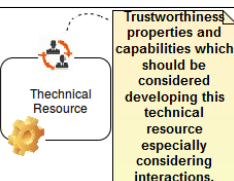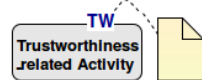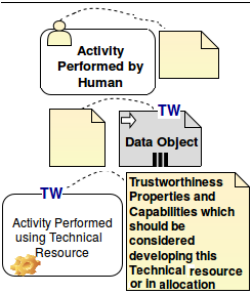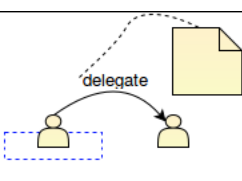
Trustworthiness elements realize the control in terms of defining elements, which directly address the trustworthiness. For instance, an additional activity can be defined to block the threat, like an activity for documenting consent or triggering a notification for a patient on delegating his/her case to another authority, or a new service from a third party is going to be used.

4.2 New Elements to Enrich the Business Process Model with Trustworthiness Requirements

We list our new elements (shown in Table 1) which are added to the business process model in BPMN to specify the trustworthiness requirements as follows:

– Monitor points: trustworthiness properties and expected behavior related to trustworthiness should be monitored. The process model must be configured before enforcing trustworthiness at run-time. We introduce the monitoring points ("*eye symbol in the model*") with start and end points in the process model for monitoring and the trustworthiness properties that must be considered in the defined monitored points, as well as the desired/target values for them. Furthermore, the metrics can also be provided for quantifying trustworthiness properties that will be under observation at run-time.

– Interaction points: these points specify the interfaces where the end-user is involved in the business process, e.g., he/she may interact with the technical resources (e.g., apps, software services) that support him/her in performing his/her tasks. In these interfaces there are factors that could signal the trustworthiness of the system to the end-user, e.g., reliability, quality of visualization, usability, understandability of represented information, quality of service, like availability or response time. For example, if the elderly person uses an app for reviewing his/her medical plan and medication, the visualization of his/her health status and medical plan influences his/her trust about the correctness of those health reports, medications or medical plans. Therefore, the trustworthiness requirements in these points ("*interaction symbol in the model*") need to be investigated further and the resources involved in these points should include related trustworthiness properties which satisfy the trustworthiness requirements.

– Trustworthiness constraints: in addition to new elements like monitor and interaction points, each BPMN element can be enriched/annotated with the constraints that they should keep for satisfying trustworthiness requirements. The action with trustworthiness requirements and constraints are tagged with "*TW*" in the business process model, e.g., time constraints on activities, or constraints on the resources which are used in performing a specific activity.

Table 1. Extended elements to model trustworthiness Requirements in BPMN

| Defined Trustworthiness Element (Extension)		Definition	Symbols
Monitor Point		Inserting monitor points into the business process defines the start and end point of monitoring at run-time. It specifies what trustworthiness-related properties are and how they can be monitored. Monitor points can be used in combination with constraints to express the desired values and metrics for measuring trustworthiness properties at run-time.	
Interaction Point		Interaction points are the places where the end-user interacts with the system. The interaction is normally supported by the apps or software services. Qualities of these apps and software services have an impact on the trust perception of users. Therefore, it should be studied well how to signal their trustworthiness to the end-user. Interaction points can be further detailed in combination with constraints on those technical resources (in interaction points), e.g., specifying which quality, to what extent (e.g., 99% availability).	
Constraint	Constraints on Activity	Trustworthiness requirements on a specific activity, e.g., expected duration of an activity.	
	Constraints on Resources	Trustworthiness requirements on a specific resource (either human or non-human), e.g., expertise of the involved human resource.	
	Constraints on Delegations	Trustworthiness requirements on delegation, e.g., if a delegation (e.g., activity delegation) is allowed, or delegation to whom or which roles are allowed.	
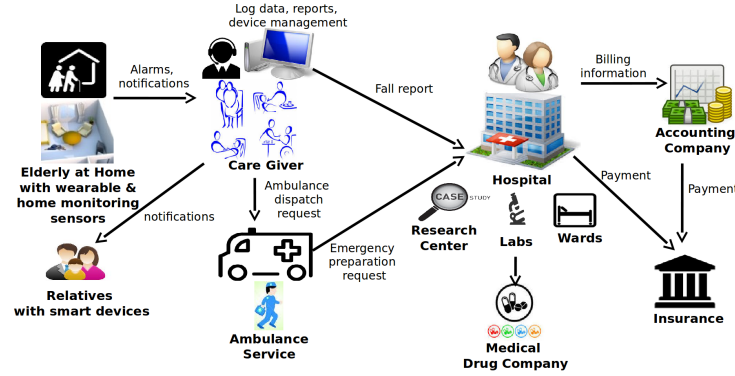
Fig. 4. The context of a home monitoring system and involved parties and actors in the scenario

5   Application Example

The example scenario presented in this work stems partially from the experience that the first author gained during the EU-funded project OPTET[1]. Figure 4 shows the context of the depicted AAL scenario.

The health care sector is an application area that has a lot to gain from the development of new ICT applications [1], [11]. Considering trust and trustworthiness of health care applications, one can consider a vector of multiple trustworthiness properties, which either address the fulfillment of the mission, e.g., reliability, safety, availability of the system when the patient needs help, response time of the service from the time that the patients request arrives until patient receives the needed health care, or from a privacy perspective. As an example, we consider a situation in the big picture scenario captured in Figure 4, where the primary requirements of the patient and the requirement on the usage of elderly's data are satisfied. The elderly person, as patient, receives his/her prescribed medicine and bills are sent to the insurance company. Hence, the usage of an elderly person's data for ordering his/her medicine or payments by insurance are allowed. However, there is a secondary usage of elderly's data which violates their desired privacy level. For instance, an elderly person receives advertisements related to his/her diseases from drug companies.

Context Analysis. Here, we illustrate the high-level view of involved entities in AAL. Such AAL systems are distributed and connected via Internet in order to support the execution of the business process. The entities consist of hospital information systems, general practitioners, social centers, insurance companies, patients, their relatives, etc. Some indicative examples of electronic medical transactions are as follows:

– Home monitoring including alarms and fall notifications,
– Emergency consultation with physician,
– Electronic notification of laboratory examination results,
– Access to the electronic medical records of patients by general practitioners,
– insurance claims.

Initially identified stakeholders in this scenario are listed below:
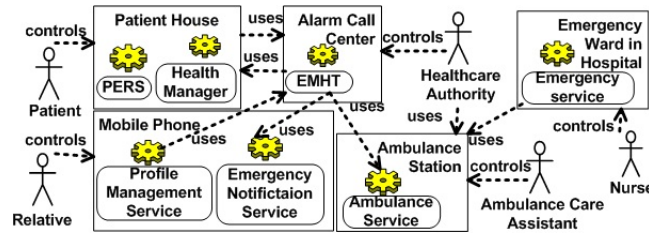
---
[1] www.optet.eu

Fig. 5. Part of home monitoring system for handling healthcare cases

- End-users: here, only elderly persons are considered as end-users (cf. Fig. 1) since they are the ones that use the offered services.
- Technology providers: These are the technology providers for medical applications like software developers (cf. Fig. 1) of home monitoring systems, fall detection systems or infrastructure providers (cf. Fig. 1) like telecommunication providers, internet service providers, etc.
- Care service provider: Health care providers, health care authorities, health care centers and clinics, hospitals are physical-service providers. These are instances of organizations (cf. Fig. 1).

Our example scenario focuses on a home monitoring system for incident detection and detection of emergency cases to prevent emergency incidents from the AAL domain. Figure 5 illustrates a general approach using supporting tools and apps, to perform the activities. We assume that some of these software services are to be built by software developers, who will also benefit from the results of our work in developing a trustworthy app, software service, etc. The Fall Management System (FMS) allows elderly people in their homes to call for help in case of emergency situations. These emergency incidents are reported to an alarm call centre that, in turn, reacts by e.g., sending out ambulances or other medical caregivers, e.g., the elderly's relatives. For preventing emergency situations, the vital signs of the elderly are diagnosed in regular intervals to reduce the hospital visits and falls.

The central asset types of the FMS include the following:

- A Personal Emergency Response System (PERS) basically consists of an alarm device which an elderly person wears so that he/she is able to call for help in an emergency situation.
- An elderly person uses the Health Manager (HM) app on his/her smart device for organizing his/her health status like requesting health service or having an overview of his/her medication, nutrition plan and appointments.
- The Alarm Call Center uses an Emergency Monitoring and Handling Tool (EMHT) to visualize, organize, and manage emergency incidents. The EMHT is a central system that receives incoming alarms from several PERS or care service requests from Health Manager apps. It gathers all relevant information related to emergency situations, health status, and supports the process of deciding and performing a certain reaction, which is performed by a human operator in an Allarm Call Center.
- An Ambulance Service is requested in case an ambulance should be sent to handle an emergency situation. The other case is that, based on analyzed information sent to EMHT, an abnormal situation is detected and further diagnoses are necessary. Therefore, the elderly person will get an appointment and notifications for a Tele-visit in his/her HM app.

Motivating Scenario. An elderly person, who lives alone in his/her apartment, does not feel comfortable after having a bad experience of a heart attack. He/she was unconscious in his/her home for several hours. The elderly person has informed the AAL services he/she considers using one of those services to avoid similar incidents in the future. Figure 6 illustrates and exemplifies the typical steps that e.g., the caregiver in the alarm center has to take once the analyzed health record of an elderly person deviates the normal situation and further examination is needed without considering trustworthiness.

The process starts by *analysing the elderly person's vital signs in the last 7 days*. These data is examined by a physician, who decides whether he/she is healthy or needs to undertake an additional examination. In the former case, the physician fills out the examination report. In the latter case, an Tele-vist is performed by this physician in which the physician informs the elderly person about examination and necessary treatment. Examination order is placed by the physician. The physician sends out a request to a clinic. This request includes information about the elderly person, and the required examination and possible labs. Furthermore, the physician arranges an appointment of the patient with the clinic for taking a sample which will be sent to the lab. Examination is prepared by a nurse of the clinic. Then, a clinic physician takes the sample. The clinic physician sends the sample to the lab indicated in the request and conducts the follow-up treatment. After receiving the sample, a lab physician validates and performs the analysis. The analysis can be done by a lab assistant. But a lab physician should validate the results. The physician from the Alarm Call Center makes the diagnosis and prescribes the medication.

Applying Proposed Approach on Motivating Scenario. Here, we demonstrate how our approach will enrich the business process model with trustworthiness requirements and then documenting those in the business process level.

Identify Trust Concerns. The elderly person is concerned about the fact whether he/she will really get the emergency help if a similar situation happens again. He/she is informed that by using this service, he/she can have regular diagnoses which can reduce frequent hospital visits. However, the elderly person is concerned if he/she will be able to use the service in proper way. The elderly person is also concerned about who can get access to the data about his/her disease or life habits. He/she indicates that he/she would only like his/her regular nurse and doctor to be able to see his/her history and health status.

Identify Trustworthiness Goals The applications of the health care domain are mission critical and privacy-related. They are mission critical, since they are monitoring the patients and dealing with the health of people. Such kinds of systems are also privacy concerned. In these systems, elderly's data are stored, processed and communicated via Internet, where the elderly's privacy can be threatened [23], [24]. We discussed the domain and application dependence of trustworthiness properties [10]. Considering the health care domain, reliability, availability, usability, raising awareness and providing guidance to privacy and user's data protection is a crucial issue related to trustworthiness [14], [1], [11], [16]. These are identified as trustworthiness goals addressing the identified trust concerns of the elderly person.
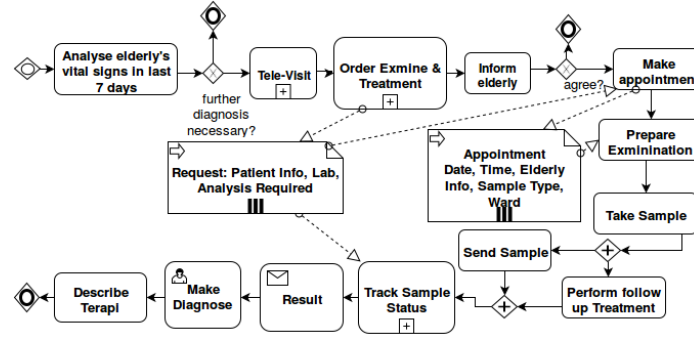
Fig. 6. Exemplary process model for analyzing elderly health situation for prohibiting emergency cases in home monitoring

Our objectives are to analyse and specify trustworthiness requirements at the business process level to support the process designers and tool developers in fulfilling trustworthiness requirements and evaluating them later. Trustworthiness constraints are defined either on the resources or activities and data objects (e.g., required expertise/experience by human resource for performing an activity) or on delegation, monitor, and interaction points (cf. Table 1).

We *select the business process model* in Figure 6. This business process is set up to fulfill the goal *"reduce number of hospital visits"*. Figure 7 illustrates the enriched business process model with the trustworthiness requirements satisfying *"reliability and privacy"*. Figure 7 shows the business process with the embedded trustworthiness requirements, which address the above-mentioned trust concerns. In particular, we exemplify the typical steps that a human resource (e.g., caregiver in alarm center) has to take or properties that a non-human resource needs to have in order to contribute to trustworthiness. We start with the activity *analyse the history of the vital signs* of the elderly person in the last seven days. This activity may detect a risk in his/her health status. The following trustworthiness requirements are specified to address the trust concerns of the elderly person related to his/her confidence that he/she is not left alone and gets the needed health care in case when necessary. Furthermore, also privacy-related concerns are specified. The elderly person should receive a regular notification that informs his/her about the diagnosis and processes that are performed on his/her
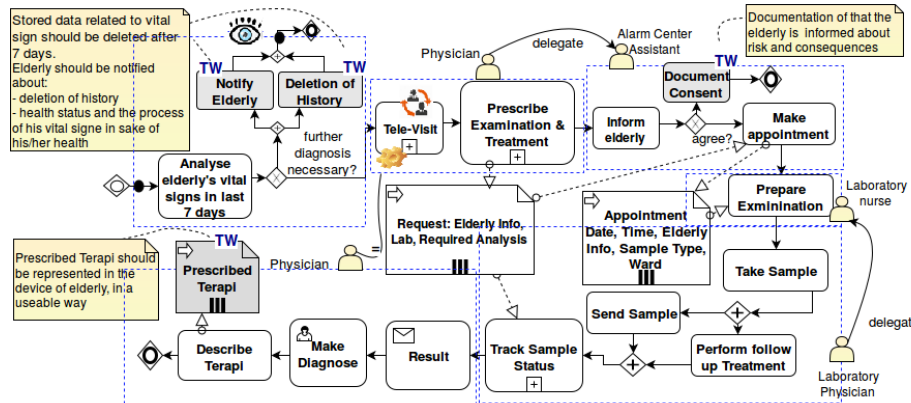

Fig. 7. Exemplary process model enriched with trustworthiness requirements and signaling controls of being worthy of trust for addressing trust concerns
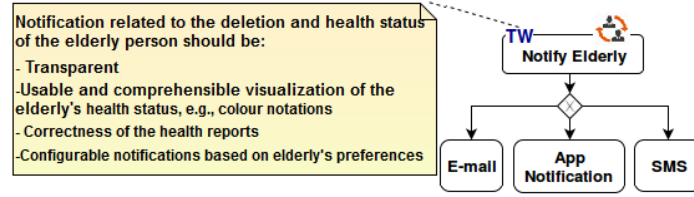
Fig. 8. Trustworthiness requirements refinement on an interaction point

vital signs. This activity contributes to make him/her confident that he/she is not left alone without care. These notifications and health status reports should be comprehensible for the elderly. If a risk to his/her health status is detected, a tele-visit is offered. This activity is an interaction point supported by the HM app as technical resource (cf. Fig. 7, tele-visit activity performed by a physician). The trustworthiness properties for this interaction point are usability, response time, etc. In case of necessity for further examination he/she should be contacted by his/her physician or responsible care assistant (delegation of physician to the assistants). Furthermore, based on history, the same physician should be assigned to activities when the elderly person is in contact with the Alarm Center staff (addressing the trust concern). After processing his/her history data and if everything is alright, his/her last 7 days of vital signs should be deleted. He/she should be still informed that the process has been performed and his/her health status is fine. He/she should be informed about the deletion of his/her history as well. Figure 8 shows the refinement on the trustworthiness requirements related to "*notify elderly*" activity. The notifications and health status reports should be understandable for the elderly person. The configurability of notification mechanisms to address the usability and privacy control in terms of intervenability is addressed. Table 2 shows the trust concerns, corresponding requirements and activities. The column *Affected Resources* exemplifies possible software design decisions on resources.

6   Conclusions and Future Work

This paper discussed trust issues in the context of BPM. In our approach, we enable the analysis of the business process from activity, resource, and data object perspectives with respect to trustworthiness.

To the best of our knowledge, we propose a novel contribution on identifying trustworthiness requirements and integrating trustworthiness properties in business process design and preparation of verification activities that satisfies trustworthiness constraints

Table 2. Examples of captured trustworthiness requirements and properties in the business process and directions on the design decisions

Trust Concerns	Trustworthiness Requirements	Activities	Affected Resources
Privacy	Transparency, Intervenability	Storage, Deletion within 7 days, Update	Private inventory system from Alarm Call Center, External cloud storage
Awareness	Usability, Transparency, Reliability, Availability	Notifications, Place appointments	App on elderly's smart device (HM)
Safety, Reliability	Reliability, Availability	Raise alarm	Redundant sensors in addition to PERS
Privacy	Correctness, Usability, Availability	Make appointment, Prescribe Examination	Elderly's details

over resource allocation and activities executions. To reduce the process designer's effort, we employ an approach for modeling trustworthiness requirements along with the business process model in BPMN. We identified the elements for specifying constraints on resources and activities that are trustworthiness-related. Then, we specify the trustworthiness requirements and constraints for those resources and activities in the business process. A solution based on data handling conditions is used to document constraints to the usage activities. The method needs to integrate fully with a business process modeling or management application. Furthermore, the approach is supported in form of a framework to support the business process life-cycle with respect to trustworthiness. The proposed approach considers the priorities of different stakeholders. However, in this paper we do not analyze whether the different stakeholders correctly report their intentions and responsibilities in the business processes. We assume a requirement engineer has already elicited the goals of involved stakeholders based on domain knowledge. In the future, we will address these issues by a method for analysis of trustworthiness requirements using goal-oriented approaches [7]. Furthermore, the social aspects of trustworthiness will be given more attention.

This is a work-in-progress paper. The main ideas and findings will be further investigated and evaluated based on the example presented in Section 5. This leads to the establishment of further patterns for formulating trustworthiness requirements [8]. Our future research will focus on three important questions: 1) It is important to understand how trustworthiness properties actually influence trust. 2) We need to understand interdependencies among different trust concerns of different parties involved in the business process, and, consequently, how to define a set of trustworthiness requirements resolving conflicts. 3) Substantial work is needed to investigate existing risk assessment methodologies on the business process level, and to show how they can support business process design and building trustworthiness into the process in its whole life-cycle.

References

1. S. Avancha, A. Baxi, and D. Kotz. Privacy in Mobile Technology for Personal Healthcare. *ACM Comput. Surv.*, 45(1):3:1–3:54, Dec. 2012.
2. J. Becker, M. Kugeler, and M. Rosemann, editors. *Process Management: A Guide for the Design of Business Processes*. Springer, 2003.
3. C. Cabanillas, D. Knuplesch, M. Resinas, M. Reichert, J. Mendling, and A. Ruiz-Corts. RALph: A Graphical Notation for Resource Assignments in Business Processes. In *Advanced Information Systems Engineering*, volume 9097, pages 53–68. Springer, 2015.
4. A. del Ro-Ortega, M. Resinas Arias de Reyna, A. Durn Toro, and A. Ruiz-Corts. Defining Process Performance Indicators by Using Templates and Patterns. In *Business Process Management*, volume 7481, pages 223–228. Springer, 2012.
5. N. Gol Mohammadi, T. Bandyszak, A. Goldsteen, C. Kalogiros, T. Weyer, M. Moffie, B. I. Nasser, and M. Surridge. Combining Risk-Management and Computational Approaches for Trustworthiness Evaluation of Socio-Technical Systems. In *Proc. of the CAiSE 2015 Forum at the 27th Int. Conf. on Advanced Information Systems Engineering*, pages 237–244, 2015.
6. N. Gol Mohammadi, T. Bandyszak, C. Kalogiros, M. Kanakakis, and T. W. and. A Framework for Evaluating the End-to-End Trustworthiness. In *Proc. of the 14th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom)*, 2015.

7. N. Gol Mohammadi and M. Heisel. A Framework for Systematic Analysis of Trustworthiness Requirements using i* and BPMN, Submitted. 2016.

8. N. Gol Mohammadi and M. Heisel. Patterns for Identification of Trust Concerns and Specification of Trustworthiness Requirements, Accepted, in the progress of publication. 2016.

9. N. Gol Mohammadi, S. Paulus, M. Bishr, A. Metzger, H. Koennecke, S. Hartenstein, and K. Pohl. An Analysis of Software Quality Attributes and Their Contribution to Trustworthiness. In *Proc. of the 3rd Int. Conf. on Cloud Computing and Services Science*, pages 542–552, 2013.

10. N. Gol Mohammadi, S. Paulus, M. Bishr, A. Metzger, H. Könnecke, S. Hartenstein, T. Weyer, and K. Pohl. Trustworthiness Attributes and Metrics for Engineering Trusted Internet-Based Software Systems. In *Cloud Computing and Services Science - 3rd Int. Conf., CLOSER, Revised Selected Papers*, pages 19–35. Springer, 2013.

11. S. Gritzalis. Enhancing Privacy and Data Protection in Electronic Medical Environments. *Journal of Medical Systems*, 28(6):535–547, 2004.

12. J. Hu. Derivation of Trust Federation for Collaborative Business Processes. *Information Systems Frontiers*, 13(3):305–319, 2011.

13. A. Koschmider, L. Yingbo, and T. Schuster. Role Assignment in Business Process Models. In *Business Process Management Workshops*, volume 99, pages 37–49. Springer, 2012.

14. H. Leino-Kilpi, M. Välimäki, T. Dassen, M. Gasull, C. Lemonidou, A. Scott, and M. Arndt. Privacy: a review of the literature. *Int. Journal of Nursing Studies*, 38(6):663 – 671, 2001.

15. H. Mei, G. Huang, and T. Xie. Internetware: A Software Paradigm for Internet Computing. *Computer*, 45(6):26–31, 2012.

16. M. Meingast, T. Roosta, and S. Sastry. Security and Privacy Issues with Health Care Information Technology. In *28th Annual Int. Conf. of the IEEE Engineering in Medicine and Biology Society (EMBS)*, pages 5453–5458, 2006.

17. OMG. Business Process Model and Notation (BPMN) version 2.0. Technical report, 2011.

18. N. Russell, W. van der Aalst, A. ter Hofstede, and D. Edmond. Workflow Resource Patterns: Identification, Representation and Tool Support. In *Advanced Information Systems Engineering*, volume 3520, pages 216–232. Springer, 2005.

19. S. Short and S. P. Kaluvuri. A Data-Centric Approach for Privacy-Aware Business Process Enablement. In *3rd Int. Working Conf. Enterprise Interoperability*, pages 191–203, 2011.

20. B. Stepien, A. Felty, and S. Matwin. A Non-technical User-Oriented Display Notation for XACML Conditions. In *E-Technologies: Innovation in an Open World*, volume 26, pages 53–64. Springer, 2009.

21. M. Strembeck and J. Mendling. Modeling Process-related RBAC Models with Extended UML Activity Models. *Inf. Softw. Technol.*, 53(5):456–483, 2011.

22. P. Sztompka. *Trust: A Sociological Theory*. Cambridge University Press, UK, 2000.

23. U.S. Department of Health and Human Services. The Health Insurance Portability and Accountability Act (HIPAA). `http://www.hhs.gov/ocr/privacy/`.

24. U.S. Department of Health and Human Services. Privacy in Health Care–Standards for Privacy of Individually Identifiable Health Information, 2001.

25. W. M. P. van der Aalst and A. Kumar. A Reference Model for Team-enabled Workflow Management Systems. *Data Knowl. Eng.*, 38(3):335–363, 2001.

26. M. Wang, K. Bandara, and C. Pahl. Process as a Service Distributed Multi-tenant Policy-Based Process Runtime Governance. In *IEEE Int. Conf. on Services Computing (SCC)*, pages 578–585, 2010.

27. C. Wolter, M. Menzel, A. Schaad, P. Miseldine, and C. Meinel. Model-driven Business Process Security Requirement Specification. *Journal of Systems Architecture, Special Issue on Secure SOA*, 55(4):211 – 223, 2009.