

# On Architectural Design of TrustMan System Applying HICI Analysis Results

The case of technological perspective in VBEs

Simon Samwel Msanjila

University of Amsterdam, The Netherlands

Email: msanjila@sceince.uva.nl

Hamideh Afsarmanesh

University of Amsterdam, The Netherlands

Email: hamideh@science.uva.nl

**Abstract:** Organizations need to trust each other for smoothing their collaboration to both acquire and respond to more and better business opportunities that none of them could do otherwise. However, in Virtual organization Breeding Environments (VBEs) there are several difficulties related to the processes that must be performed to facilitate organizations create trust to each other. The main cause of these difficulties is the way these processes are currently performed which in most cases are ad hoc and manual. Among others the processes include: assessing trust level of organizations, creating trust among organizations, establishing trust relationships, and managing trust related data. As a result, configuring virtual organizations (VOs) within the VBE environment is becoming challenging and difficult. To match the pace in the market these processes must be quickly performed and must produce very accurate results. Thus they must now be supported with semi-automatic systems. In order to properly assess trust level of organizations in VBEs, trust elements and trust relationships must be thoroughly characterized. This paper addresses the characterization of trust elements and automation of processes related to the management of trust among organizations. It presents a three-stage approach for identifying and analyzing trust elements. The identified trust elements and their related analysis results are then applied in the design of mechanisms and architectures for Trust Management (TrustMan) system. The design of two architectures (operational and componential) for TrustMan system is also presented in this paper.

**Index Terms:** HICI, Trust elements, TrustMan system, VBE

## I. INTRODUCTION

The market is now continuously evolving to match the today's connected and digital world. The organizational preparedness needed to facilitate collaboration initiatives must match the market's evolution [22]. One important aspect of preparedness to enhance collaboration among organizations is creating trust to others. To match the needed pace in the market the processes to be performed for creating trust among organizations must now be semi-automatic and supported with some management systems.

However looking at today's digital world, until a few years ago, enhancing security of information, resources, stored knowledge, available skills, etc., was a fundamental approach to assure trust which also distinguishes between organizations dealing with information and communication technologies (ICT) and business organizations. Due to increasing challenges related to required security the organizations dealing with ICT started to ask questions about bits and bytes, key lengths, signatures, certificates, etc. However, business organizations were only looking at opportunities to maximize their profits and market coverage. Nonetheless, with time the situation has changed dramatically: new regulations, significant security, privacy incidents, etc. are not enough to assure smooth operations for networked business organizations in the current market which is witnessing continuously increasing turbulent conditions.

From a business view, security is mostly about managing risks, and in this case related to ICT facilitative tools. The current market is characterized with turbulent conditions, such as among others: scarce resources, lack of knowledge and skills, volatile business opportunities, changing and emerging unique customer requirements, etc. Enhancing security and managing risks do not guarantee organizations' success and survivability in today's market.

An ICT system can provide the right level of security whether or not it keeps the risks for business at an acceptable level. What counts for this risk in relation to security, are the potential losses due to ungentle acts by disgruntled employees, hackers, unauthorized users, etc. Whether a risk is acceptable or not is a business decision and is hardly influenced by the state of the ICT system [22]. To describe the security or risk level and to demonstrate that an ICT system meets that level is a fundamental challenge in current research. It is more challenging today as organizations must collaborate to together acquire and respond to opportunities which need geographically distributed support from ICT systems.

Security had been getting attention in the past but securing ICT system is becoming more difficult than ever. The dependencies among organizations are rapidly growing: the increasing specialization in industry to enhance market focus, the increasing needs for cooperation among organizations to respond to specific business opportunity, etc. These dependencies are however becoming more and more dynamic. Cooperation and collaboration is becoming palpable for organizations' survivability in the current market [13]. Security alone is not enough to smoothen the cooperation and collaboration and thus guaranteeing the needed successes. As a result, the security boundaries among organizations are quickly becoming less and less strict. Applications that used to run on dedicated machines now run on virtual environments, shared infrastructure, and using resources that might be spread all over the world [17].

Because of growing complexity of problems related to security of ICT systems, risks associated with businesses, market turbulences, etc., some other approaches for smoothing the operating environments are needed and must be looked upon, and especially considering the today's fundamentality of cooperation and collaboration among business organizations. Managing trust among organizations by applying rational mechanisms for assessing trust level and creating trust has emerged as one of the promising approaches for providing the required smoothing [20]. A number of processes need to also be automated to provide the needed semi-automatic services for management of trust among organizations (section V). All aspects of trust and all measurable trust elements (trust criteria) as identified in this paper by applying the HICI approach (section III) must be considered while formulating the mechanisms for assessing trust level as well as automating the related processes [22].

Once in a network or alliance, such as in a VO or in a VBE, organizations need suitable approaches and semi-automatic mechanisms to evaluate trust level of others and to establish trust relationships to each other [23]. When properly characterized, a challenging task on its own, member organizations in the VBEs will be able to assess and measure trust level of others. Trust relationships among organizations are central to the successful operation of VOs and VBEs, as well as the effectiveness of their administration. In this paper we apply the following definitions for VOs, and VBEs:

*A VO is an association of (legally) independent organizations, such as VBE members, that comes together to share resources and skills to achieve a common goal such as acquiring and executing a collaboration opportunity [13].*

*A VBE is defined as an association of organizations and related supporting institutions adhering to a base long term cooperation agreement, and adopting common operating principles and infrastructures, with the main goal of increasing both their chances and preparedness towards collaboration in potential VOs [8].*

One important aspect of characterizing trust in VBEs is identifying trust elements for its various organizations. *We define trust elements as the hierarchical-related elements from abstract (non measurable) ones which represents the root node to the measurable ones which*

*represent lowest child nodes that together characterize both trust and trust relationships, and form the base for deciding about the data needed for the rational assessment of trust level of organizations [20].* Some trust elements defined in the literature for organizations are subjective (opinion-based) and thus cannot be measured or reasoned [2]. But performance based trust elements can also be identified for organizations that are fact-based and are measurable as addressed in this paper.

In order to solve trust assessment problems, organizations had been applying ad-hoc approaches to identify trust elements and use them in measuring trust level of others. Nonetheless, none of the current practiced approaches and mechanisms is generic and in most cases they lack the reasoning behind the resulted trust levels [20]. These approaches are sometimes application dependent and thus can be applied only to specific application such as for the establishment of trust relationships in health care, for government services, etc. The approaches are sometimes domain dependent that can be applied to specific kind of information about organizations, such as their financial records, technical capacities, etc. It is also complicated since these tasks are handled manually and in ad hoc manner [22]. Thus the practiced approaches are inadequate to address trust aspects as need to be characterized in VBEs.

In VBEs, in addition to the need to automate processes related to the management of inter-organizational trust, trust requires to be characterized as a multi-objective, multi-perspective, and multi-criterion subject [24]. In this paper we address the subject of trust among different actors in VBEs and specifically, the challenging tasks of how to identify trust elements, analyze the inter-relations with each other and automate tasks related to managing inter-organizational trust in VBEs. We introduce the **HICI** (**H**ierarchical, **I**mpact and **C**ausal **I**nfluence) approach for the identification of trust elements for organizations in VBEs and present architectures for TrustMan system. The presented architectures apply the trust elements and specifically the trust criteria for the formulation of mechanisms for the TrustMan system.

#### A. Definitions of base trust concepts

Below in this sub-section, the definitions of base concepts of trust as used in the paper are presented [20].

- **Trust actors:** Refer to the two organization parties involved in a specific trust relationship. The first party is the organization that needs to assess the trustworthiness of another and is referred to as the trustor. The second party is the organization that needs to be trusted, and thus its trust level is assessed and is referred to as the trustee.
- **Trust objective:** Refers to the purpose for which the trust relationship establishment among involved organizations is required.
- **Trust perspective:** Represents the specific "point of view" of the trustor on the main aspects that must be considered for assessing the trust level of the trustee.
- **Trust requirement:** Represents the essentials (cardinals) that characterize and guide on how the respective trust perspective can be realized. Thus, trust requirements are the fundamental cardinals that guide or suggest what must be met in order for the respective trust perspective to be

realized. E.g. “financial stability” is an example requirement that must be met to support the economical perspective, etc.

- **Trust criteria:** Represent the measurable trust elements that characterize a respective trust requirement. For each organization, the values of its trust criteria can be used to make a rational (fact-based) judgment on whether the respective requirement is met. The only source of data for trust criteria is the respective trustee organization but the data must have validity evidences. After joining the VBE, the main source of data for organizations becomes the performances from their participations in VOs.
- **Known factor:** Represents a set of domain/application dependent factors that indirectly influence the outcome of measurements of trust level for the involved organizations. Each domain/application, such as business, manufacturing, medical, etc. is affected by both VBE’s internal factors (e.g. the minimum wage per hour for all organization within the VBE), as well as the VBE’s external factors about environment / market / society considering the VBEs scope both geographical and area wise, such as some pre-existing regulations or standards (e.g. regional tax subsidies), some environment’s norm (e.g. minimum number of competencies required to join a VBE member), etc. The only source of data for the known factors is the administration that knows about both environments.
- **Trust level:** Refers to the intensity level of trust for a trustee in a trust relationship, based on the assessment of values for a set of necessary trust criteria. Clearly enough, the criteria for the trust level assessment of organizations are varied and wide in spectrum depending on the purpose (e.g. depending on the requirements, the perspective, and the objective of trust establishment). When trust level is assessed for a certain specific purpose, such as for inviting a member to a VO and the assessment is based on specific trust criteria for that specific purpose, we call the results, specific *trustworthiness* of the trustee.

**B. Problem area and research questions**

Trust is defined differently in different disciplines and research and following definitions are dominant:

- *Trust is the willingness of a trustor to be vulnerable to the actions of another party based on the expectations that the trustee will perform a particular action important to the trustor irrespective of the ability to monitor or control the trustee [16].*
- *Trust is the belief in the competency of an entity to act dependably, securely and reliably within a specified context [26].*
- *Trust is a psychological condition comprising the trustor’s intention to accept vulnerability based upon positive expectation of trustee’s intentions and behavior [3].*

The diversity among these definitions makes it difficult to properly characterize trust and its concepts. There are many theories on trust, some of which diverge from each other only in their identification of the grounds on which they are based [3]. Despite the difficulties in solidifying the definitions of trust, it is a base for collaboration among individuals and among organizations. Research on collaborative networks already reported that the effectiveness of VBE as well as the VO depends on the right balance of trust level among organizations [21].

*In this paper we define trust among organizations, as it is applied in VBEs, as the objective-specific confidence of a trustor to a trustee based on the results of rational (fact-based) assessment of trust level of the trustee.*

Therefore, objective based trust creation refers to the process of creating trust among organizations based on

the results of the rational assessment of their trust levels. Only measurable or numeric data are applied here and the resulted trust levels can be supported with some formal reasoning, such as mathematical equations, applied in formulating mechanisms for assessing the trust level of organizations, which in turn enhances the reasoning of the established trust relationships [20, 23]. While the importance of trust relationships is palpable for collaboration among organizations, the following series of questions must be properly addressed:

*a) Can trustworthiness (trust level) of an organization be measured? How complex is trustworthiness? Does it have a quantitative value, and if so, what is the metric? Furthermore, is it one number or a set of numbers? If not quantitative, then is it a qualitative value, such as good/bad, high/ low?*

In [20] we presented an approach for measuring trust level of organizations in terms of values for a set of trust criteria. We argued that trustworthiness is complex and can neither be measured with a single value nor interpreted with a single metric. The levels upon which the organization’s values meet the specified comparative ratings set by the trustor represent its trust level.

*b) Does every organization have the same objectives and perspectives for establishing trust relationship with others?*

In VBEs, trust must be characterized to facilitate the understanding of the purposes that motivate organizations to establish trust relationships. It should also be studied to understand whether these objectives are similar or different as well as whether their primary aspects for establishing trust relationships are uniform. This paper addresses this question.

*c) Which trust criteria and how many must be applied to measure trust level of an organization?*

In order to properly assess trust level of VBE member organizations measurable trust elements must be comprehensively identified, their inter-relations analyzed, and their impact on the trust levels studied. We also address this question.

*d) How to automate tasks related to the management of trust among organizations in VBEs?*

In [22] we addressed the specification of TrustMan system and how those specified functionalities could assist the management of VBEs. In this paper and in relation to the automation of the management of inter-organizational trust we address the design of architectures for TrustMan system applying the rational trust elements identified by applying the HICI approach.

The remaining part of this paper is organized as follows: section II addresses the aspect of technological perspective for trust among organizations. Section III presents the suggested HICI approach. Section IV addresses the customization of trust elements for a specific VBE. Section V presents the architectures designed for TrustMan system. Section VI addresses the execution paths and experimentation of the system. Section VII concludes the paper.

**II. TECHNOLOGY AND TRUST IN VBEs**

This section addresses technological perspective. First it provides an overview of trust perspectives for VBEs.

### A. General trust perspectives

Trust is a key concept addressed by research in different disciplines and has increasingly gained importance in the emerging info-society. In Table I we list the perceptions in some disciplines [20].

TABLE I. PERCEPTIONS OF TRUST IN DIFFERENT DISCIPLINES

Discipline	Perception
Sociology	Reputation and interactions
Economic	Decision about risky choices
Psychology	Beliefs
Politics (government)	Truth telling
Computer science	Security, reputation, & privacy

In [24] we identified five trust perspectives for creating trust among organizations involved in VBEs, namely: *structural, social, economical, managerial, and technological perspectives*. To assess the trust level of trustees, trustors may opt for some or all perspectives depending on their specific trust objectives. Here, we use the technological perspective to exemplify the HICI approach for identifying fact-based trust elements for organizations participating in VBEs.

### B. Technological perspective

The emerging economy is knowledge-based and without borders, where the competition is among organizations - local and international - on how to learn faster and organize more flexibly to take advantage of "technology-enabled" market [6]. Within this new economy, the information and communication technologies (ICTs) are ubiquitous. They have transformed geographically separated locales into a "global village" for information sharing, organizational interactions, and exchange of economical value. Technology, in particular, ever-expanding digital bandwidth, has resulted in creation of new economy forms of intangible, knowledge-based capital, the value of which now exceeds that of the physical capital that dominated old economies [24]. Whereas business models for old economy emphasized tasks and roles organizationally, business models for the new economy focus on self-organizing: teams, companies, and industry-based clusters, or collaborative networks (CNs). Organizations have now realized that by working in collaboration, such as in CNs, they enhance their chance to jointly meet continuous changing requirements of "innovation-demanding" opportunities more effectively [13]. There are three main questions to address when thinking about technology in the new economy:

- *What are the distinguishing factors, which separate ICT-enabled collaboration in physical from virtual settings?*
- *Can findings from physical collaboration help to understand the emerging virtual collaboration?*
- *How does the creation of trust differ for physical collaboration and for virtual collaboration?*

ICT-enabled physical collaboration is a technology-based collaboration with the presence of some level of face-to-face communication. It also refers to an electronically supported communication media ranging from telephone to Internet, to low-earth orbit satellite and

cellular technologies that organizations use to support linking them to others [12]. The main concept here is the synchronous communication. For example, the meta-analysis of twelve studies presented in [4] suggests that electronically supported face-to-face meeting tools, such as group support systems, influence: decision quality, time to reach decisions, participation quality, and degree of task focus. In an empirical study in [6], it was found that audio conferencing may be substituted for and can even outperform face-to-face meetings. However, face-to-face meeting was found more effective than audio conferencing for tasks which need extensive interactions and are complex in nature [4].

Moreover, the world has witnessed a shift from immobile-wired infrastructures to mobile, miniature, and wireless modes of communication, computing, and transacting. Customers demand "any time, any place" solutions for their problems. Such demands have led organizations to invest in creating online business processes and services as either substitutes or supplements to brick-and-mortar service offerings [19]. Also, due to increasing need of reducing time cycles for satisfying customers, organizations now face hard challenges in adapting their human resources and practices to the fast-moving business. Organizations with rigid plans will destroy their economical value when market and technologies advance [27].

Innovative organizations that employ technology to facilitate collaborative projects are the hallmark of the new economy [24, 14]. Such collaborations can range from arms-length information sharing to highly interdependent and geographical dispersed joint projects. In large VBEs, organizations cooperate/collaborate with others that sometimes are physically unknown to them. These organizations must trust each other in order to effectively work together. Basically, in the current innovative-based economy trustees must possess the technology which can facilitate the co-working.

Moreover, the current economy demands ability to acquire and possess competitive information and knowledge. Technologies are playing a great role in achieving such organizations' goals efficiently. The number of domains where technical artifacts are filtering organizational communications and relationships is increasingly growing: computer supported interactions, computer supported co-work, e-commerce, or even e-mails are just few examples of this trend. The importance of trust, considering the technology side, is twofold: (1) it can be seen as trust towards the technical system (i.e. in electronic payments), and (2) trust in the technology as a mediator among actors. Therefore, when setting-up collaboration, organizations that possess required technologies are assessed technologically trustworthy.

*Therefore, we define technological trust, or trust based on owned, applied or experienced technology by an organization is an objective-specific confidence based on the results of trust level assessment which applied rational technological data to indicate the capability that the underlying technology (infrastructure) can facilitate interactions or transactions as required [21].*

In this point of view, to achieve high trust level, the trustee must possess a good ICT infrastructure to facilitate the collaboration as well as the specific required technology for running the business opportunity. For some purposes, trustors may consider technology as primary aspect, or in combination with others, when assessing trustees' trust level based on technological performances (Table II).

*C. Trust versus privacy among organizations*

At individual level privacy can be seen as a fundamental human right. Similarly, organizations are now facing the problem of privacy and specifically, in relation to confidential data and strategies. Different mechanisms have been proposed to protect the privacy of organizational data in the world of computers, both legislative and technological, depending on whether privacy is seen as a right, which should be protected by laws or a need, which should be supported by devices. From the privacy point of view and considering interactions among organizations, there is an inherent conflict between trust and privacy: the more knowledge a 1<sup>st</sup> entity gains about a 2<sup>nd</sup> entity, the more accurate will be the result of trust level assessment. But the more knowledge is gained about the 2<sup>nd</sup> entity, the less privacy is left to this entity [11].

*D. Trust and security among organizations*

There has been a misconception about trust and security, and the role that technology plays in this binomial for setting/facilitating collaboration. Most people tend to believe that trust is merely the result of security - when it is secure, actors can trust each other - but researchers have observed that this is not the complete picture [3]. Trust is a wider concept and its link with security is not linear [23]. Technology can effectively provide security: every step of an online transaction has one or more procedures for transmitting users' data safely, i.e. cryptography, protocols, etc. This does not mean trust though. Security driven approaches for creating trust among organizations have led to a bias that named "the double illusion of 100% safe" [5].

It is said that technology is always deceptive: it is safe until it is violated. Every secure environment will soon become insecure, because technical innovation works on both the good side of security protocols and on the bad side of hacking processes. Technology can only make this breaking moment as far in time as possible [26]. Organizations that assume the security of the environment, which is enhanced by the technology, as the only means to trust others might face difficult when unexpected problems occurs, such as hacking of software [23]. This is the first illusion.

Consider a moment that a secure environment is maintained. Organizations can act freely and confidently because they are protected by technology. However this is not a trust building atmosphere because the importance of trust increases when there is a chance of some risks happening [11]. An environment depicted with hard technology protection deteriorates trust building:

organizations feel the security but not necessarily the trust. This is the second illusion.

*E. Trust criteria for technological perspective*

In addition to security and privacy a number of other important trust criteria for organizations related to the technological perspective must be identified and characterized. We have observed that the role of technology in VBEs should be re-contextualized: it is without any doubt an important element that must be considered within trust strategies especially for the collaborative businesses [23]. Technology can have a background role: it is fundamental to achieve a solid base of security and robustness for infrastructures. Without a proper and functioning infrastructure organizations can hardly interact in technologically enabled environment. But after this initial role, trust should be handled by considering the use of technology in enhancing organization's abilities such as its technological related performance, etc. For exemplification purpose Table II introduces some subordinate trust elements for technological perspective identified by applying the HICI approach which is presented in section III.

TABLE II. SUBORDINATE TRUST ELEMENTS FOR TECHNOLOGICAL PERSPECTIVE

Requirements	General trust criteria
ICT- Infrastructure	Network speed
	Interoperability
	Availability
Technology standards	Protocol supported
	Software standards
	Hardware standards
Platforms	Security standards
	Operating systems
	Programming languages
Platform experience	Applied in VOs
	External project applied
	Duration held

III. HICI: IDENTIFYING TRUST ELEMENTS

Our approach that we present in this paper constitutes three main concepts, namely: **H**ierarchical, **I**mpact and **C**ausal **I**nfluence analyzes and thus this approach is called HICI. The three main concepts constitute this three-stage approach for identifying trust elements and analyzing their inter-relations as addressed below.

*A. Stage I: Analysis of hierarchical relations*

The hierarchical relations defined among the trust elements represent their inter-relations from a highly abstract element (e.g. trust objective) to its subordinate measurable elements (trust criteria). We have identified here five levels of abstraction (L1 to L5) for representing the hierarchical relations among trust elements (Fig. 1).

The establishment of each trust relationship is for a certain objective. The *trust objectives* (e.g. for creating trust among organizations) characterize the reason *why trust relationships must be established*. Each trust objective is further characterized by a number of *trust perspectives*. Furthermore, each trust perspective is

characterized by a set of *trust requirements*. Each trust requirement is also characterized by a set of *trust criteria*. Each trust criterion constitutes a value structure (Fig. 1).

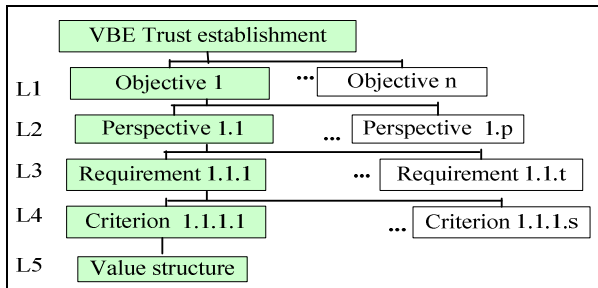


Figure 1. Hierarchies among trust elements for organizations.

Following the steps in stage I, starting with the trust objectives, trust elements can be identified and characterized as shown in Fig. 1. Applying the hierarchical analysis as addressed in this stage and involving some VBEs including: IECOS, Virtual Fabric, CeBeNetwork, ISOIN (www.ecolead.org) for validation purpose, we have identified a set of trust elements for the three trust objectives (TB) as follows:

**TB1: For creating trust among organizations:**

Five trust perspectives that can be preferred by a trustor for creating trust to trustee were identified, namely: structural, economical, technological, social, and managerial perspectives. Fig. 2 shows a comprehensive set of general trust elements.

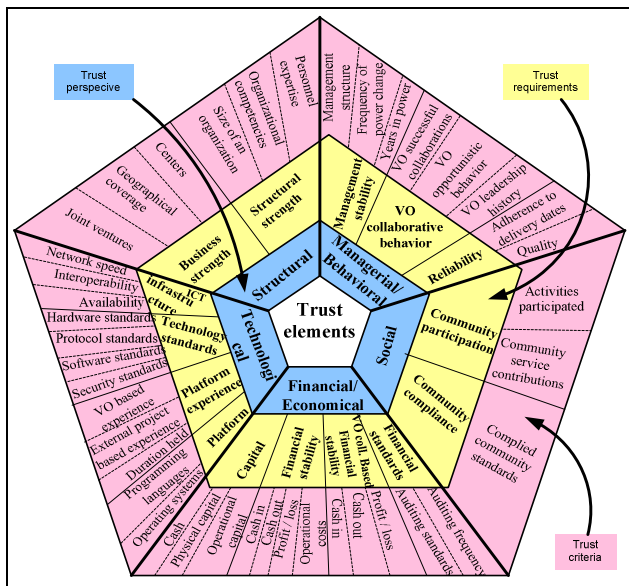


Figure 2. Hierarchies among trust elements.

**TB2: For creating trust of a member organization to the VBE administration:**

A VBE member organization needs to be convinced that the VBE administration is trustworthy in order to join and remain active in the VBE. For example, since the VBE member organizations are continuously competing to win chances for participating in VOs within the VBE, they must be convinced that the administration is impartial and that the selected members for each VO are

chosen based on their qualifications. Below we address four trust perspectives (summarized in Fig. 3) and provide their subordinate trust elements.

- *VBE policy related perspective:* VBE policy addresses the plan of action to guide VBE decisions and activities. Policies can be understood as political, management, financial, and administrative mechanisms applied for reaching goals. For VBEs, the main aspects related to trust, and the policies that must be accessible to member organizations are shown in Fig. 3.
- *Transparency and fairness related perspective:* The VBE administration must be transparent and fair to all member organizations. In specific, some of the main transparency issues sensitive here refer to the steps taken or activities performed for the entire process of assessing the trust level and measuring the performance, which are in turn the key sources of trust related data (Fig. 3). Fairness refers to the fact that as much as possible there should be unified formal reasoning mechanisms and approach for decisions made in the VBE.
- *VBE component related perspective:* Refers to the components that constitute the VBE. The main components of a VBE are: member organizations, and supporting institutions. A member organization that wants to assess the trustworthiness of the VBE and its administration will need the information related to VBE structure and its components (Fig. 3).
- *VBE-self related perspective:* When it comes to trusting the VBE, member organizations of the VBE must also be provided with the information that can build a positive picture about the VBE as whole. Here the relevant information needs to address performance of VOs and other information about VBEs that are restricted for its member organizations, as shown in Fig. 3.

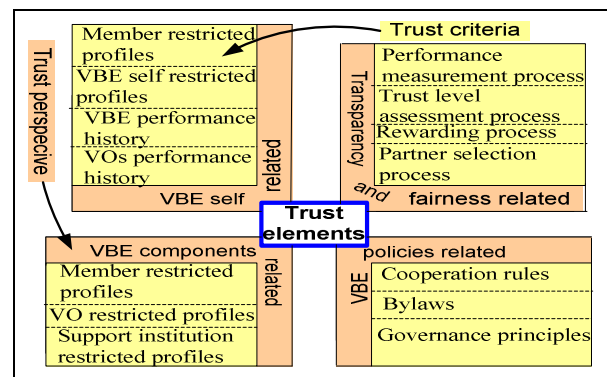


Figure 3. Trust elements for trust of members to the VBE administration.

**TB3: For creating trust of an external stakeholder to the VBE:**

External stakeholders must be convinced to trust the VBE. For example, in order to select the VBE (e.g. when a customer wants to provide a tender, etc.) customers will need to trust the VBE. Also an invited organization needs to trust the VBE before deciding on becoming a member. In this paper, we recommend providing these stakeholders with the information related to the following three specific trust perspectives (Fig. 4):

- *Profile related perspective:* This information will enable the external stakeholder to understand the constituents and competencies of the VBE.
- *VBE advertisement related perspective:* As in normal business world, VBEs will also advertise their products

and services to the market. Information on advertisements that are usually made can indicate the capability of the VBE to support its members for business opportunity brokerage and its capability to reach its customers.

- Service for client related perspective: An external stakeholder, such as a customer, can be convinced to trust the VBE based on the availability of the services that it needs and the quality of the VBE support for service acquisition.

The rational assessment of the organization’s trust level as applied here is based on their past performance. Thus, the trust levels of organizations are rationally measured. In order to properly and rationally assess the trust level of organizations the relations between the trust criteria and performance of an organization as well as the inter-relations among the trust criteria must be thoroughly studied as addressed in the next two stages.

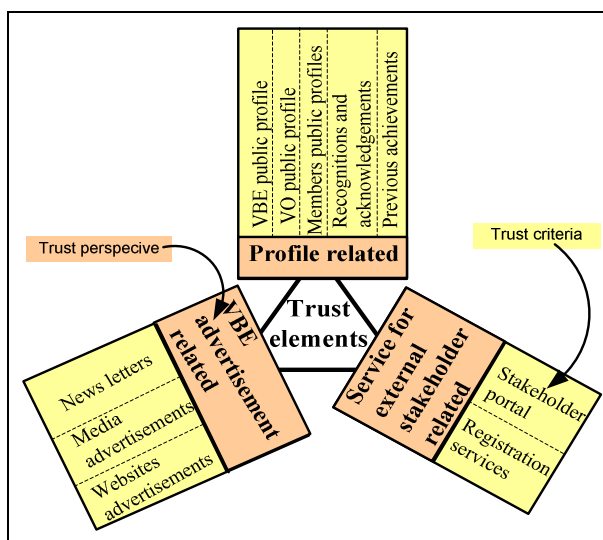


Figure 4. Trust elements for trust of external stakeholder to the VBE.

**B. Stage II - Analysis of impacts relations**

Trust criteria, which are the base for the measurement of trust level, are not “directly” related to the organization’s performance. Thus some “intermediate factors” exist. *Intermediate factors represent the factors that play the intermediary role in relating known factors to the trust criteria.* In principle, both trust criteria and known factors do influence each other. Their influences are twofold: causal and impact influences that both arise through the intermediate factors. In stage II, impact analysis enables both the identification of these intermediate factors and the proper analysis of their relations to the trust criteria, and to the performance.

To further describe this concept, consider the technological perspective as in Table II. With an empirical study of the organization’s domain, and validated by the domain experts, we have identified some intermediate factors, in order to present our example for the impacts analysis. Fig. 5 shows how changes in the values of trust criteria for the technological perspective create impact on intermediate factors that can improve organization’s performance which enhances trust level.

For example, consider an organization that possesses and deploys an ICT-infrastructure, which is widely used in several organizations,

and it has high: speed, interoperability and availability. The technology also qualifies several standards, e.g. protocols, security, etc. Thus the organizations can smoothly facilitate the set-up of technology-based collaboration. Also, it will enhance its common communication context as well as increase its connections to other. If these are achieved then communication to partners both direct and indirectly will be enhanced. Thus it will facilitate the sharing of some new ideas and information, which in turn will facilitate re-use of existing technical solution in the network, and thus reducing the learning curves which in turns will improve its performance and hence enhance the trust level.

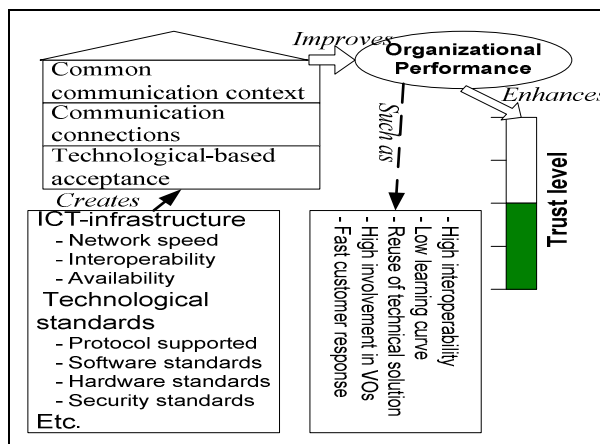


Figure 5. The impacts of trust criteria on performance.

**C. Stage III: Analysis of causal influences**

To address trustworthiness as a fact-based measurement, it is causally related to the past recorded events and actions that an organization performed. These relations are not direct and in most cases there is a lack of important and complete data necessary to reason about them. In order to analyze and build good understanding about causal influences and their impacts on trust levels, approaches that support reasoning with partial/incomplete data are needed [27].

In [20] we described in details how causal analysis and reasoning as inspired in system dynamics discipline can be applied for the analysis of trust level. Basically, we apply causal analysis to study the variation of performance of an organization based on the behaviour of values of trust criteria. The behaviours of these trust criteria do influence each other as a system. For example, the behaviour of one trust criterion can influence the behaviour of several others. Also, some influences are exerted to the system from external environments.

Understanding essentials of the causal model requires suitable knowledge of the context within which it was developed and applied [15]. Causal modeling approach does not have standard factors that are typically considered for any modeling. Thus factors that are included in a certain causal model are widely varied and dependent upon: *the modeler, problem addressed, domain, stakeholders, etc.* In stage III we use causal analysis first to understand the influences among trust elements, organizations’ activities, and the environments, and second to identify impacts on the trust level based on their causal behavior. Since the assessment of organization’s trust level depends on values of these trust criteria, changes in these values will also causally



trust criteria, known factors and intermediate factors. The derivations of equations are beyond the scope of this paper but they are presented in detail in our previous publication [20]. Below are three general formulas as applied in TrustMan system [22].

$$TL = Avg[(W_{Tech} * S_{Tech}), (W_{Soc} * S_{Soc}), (W_{Str} * S_{Str}), (W_{Man} * S_{Man}), (W_{Eco} * S_{Eco})] \dots (1)$$

$$S_{per} = \frac{1}{n} \sum_i^n W_{IF_i} * S_{IF_i} \dots (2)$$

$$S_{IF} = f[\text{trust\_criteria, known\_factors}] \dots (3)$$

Where  $0 < W_i < 1$ , and  $\sum_{\forall i} W_i = 1$

*TL: trust level, S: score, per: trust perspective, IF: intermediate factor, W: weight, Avg: average*

**B. Specification of TrustMan system**

In [22] we presented the specification of TrustMan system addressing the users, requirements, functionalities and technical environments. Six functionalities (services) were specified for TrustMan system as follows:

1. *Assessment of base trust level:* A service providing support for assessing the minimum acceptable level of trust for an organization to remain a member in the VBE. A set of base trust criteria is applied for the assessment.
2. *Evaluation of specific trustworthiness:* A service providing support for evaluating specific trustworthiness of organizations for an emerged objective. A set of specific trust criteria is applied for the evaluation.
3. *Establishing trust relationships:* A service providing support for establishing trust relationship among organizations by providing information that will enable involved actors to trust each other.
4. *Creation of trust to the VBE:* A service providing support to the external stakeholders to create their trust to the VBE.
5. *Management of trust related data:* A service providing support to the VBE administrator to manage the data in TrustMan system applied for the assessment of trust level of member organizations.
6. *Management of TrustMan mechanisms:* Mechanisms implemented for TrustMan system apply mathematical equations. The parameters included in these equations do have some weights depending on the preferences of Trustors. This service provides support to trustors to change these weights based on their preferences.

**C. Architectures for TrustMan system**

In this section we present the architectures for TrustMan. We first present the operational architecture and then the componential architecture.

**Operational architecture for TrustMan system:**

TrustMan system is one of the subsystems that together constitute the so-called VBE management system (VMS). The VMS is designed to assist the VBE administration

to semi-automatically perform the managerial related tasks. In this regard, TrustMan system assist the VBE administration with handling the tasks related to managing trust among organizations in the VBE. To properly and comprehensively provide the required services TrustMan system interacts with others sub-systems for four general purposes, namely: (1) for acquiring the trust related data, (2) for providing results from the trust level assessment, (3) for accessing ICT-Infrastructure (ICT-I) basic services, and (4) for supporting human access. The architecture as shown in Fig. 7 represents the operational architecture for TrustMan system.

*1) Interactions for acquisition of trust related data*

Two sub-systems namely: *Membership Structure Management System (MSMS) and Performance Data related Management Systems (PDMS)* interact with TrustMan for submitting trust related data (Fig 7).

MSMS is designed and implemented to support the VBE administration with handling tasks related to registration of new VBE member organizations and defining their respective roles and rights in the VBE. One of the key information, which is necessary for the VBE administrator to decide about the acceptance of the VBE membership applicant, is its base trust level. In order to assess the base trust level of the applicant organization its trust related data, represented in terms of values for trust criteria, must be submitted to TrustMan system for all base trust criteria. Thus the MSMS interacts with TrustMan system to facilitate the applicant organization to submit its trust related data to the TrustMan system.

While the VBE is in operation phase its member organizations participate in a number of activities, both within the VBE and in configured VOs. Thus their trust related data in the TrustMan system must be continuously updated. The main source of trust related data is the organizations' performance made in those activities. Therefore, the PDMS interacts with TrustMan system to assist the VBE member organizations or VO coordinator with updating the trust related data in TrustMan system based on the performance data of organizations collected from their participation in the VBE and in VOs. The PDMS includes set of sub-systems for managing VO information, inheritance, VBE related performance, etc.

*2) Interactions related to accessing trust level*

Some VMS subsystems need to invoke a number of services provided by TrustMan to access the records of trust level for organizations. The trust levels of organizations in this case are used as input towards providing the required services by those subsystems to their users. Three VMS subsystems are identified, namely: *MSMS, Decision Support System (DSS) and Partner Search and Suggestion (PSS)*.

The MSMS invokes the service for assessing base trust level of membership applicant for the aim of analyzing whether the applicant organization meets the specified minimum level of trust in the VBE. Thus the MSMS uses the resulted trust level as one of the key information

together with other information, i.e. competency analysis results, etc., for deciding on acceptance of application.

The DSS supports the VBE administration with making decisions on a number of issues but mainly in relation to controlling and alarming member organizations for: the VBE competency gap, the organization's lack of performance, and the organization's low trustworthiness. Specifically for this case, in order to analyze the deteriorating trust level of the organization the DSS invokes the services provided by TrustMan system for assessing base trust level of organizations. The interactions take place in scheduled manner and thus the organizations whose trust level is continuously falling are alerted and advised on how they can enhance their trustworthiness.

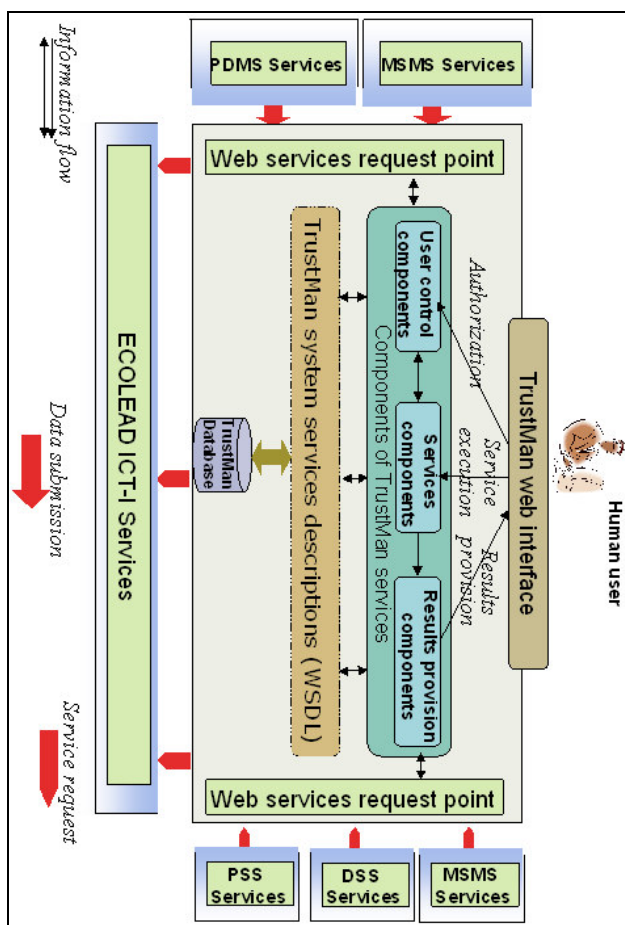


Figure 7. Operational architecture for TrustMan system.

The PSS supports VO planner with selecting potential VO partners among the VBE member organizations for inviting them into a VO which will be configured to respond to a brokered opportunity. One key activity during the selection of potential VO partners is the evaluation of their specific trustworthiness. Thus the PSS interacts with the TrustMan system to facilitate the VO planer with evaluating the specific trustworthiness of potential VO partners.

3) Interactions for invocation of ICT-I basic services

The TrustMan system needs to invoke basic services provided by the ICT-I to properly function and provide

required services for trust management. There are a number of basic services provided by the ICT-I developed in the ECOLEAD project. The TrustMan system needs to invoke and use two basic services from the ICT-I, namely: *the services for data access, and services for security management.*

The service for data access supports the TrustMan system with handling the performance data in its database, such as updating and retrieving data, and especially related to the interactions with the MSMS and PDMS, etc. The service for security management supports the TrustMan system with authentication of user and specifically, the remote users. It involves authenticating source networks, security certificates, etc. to maintain the required security for the TrustMan [22].

4) Interactions related to the human access

The interactions between human users and the TrustMan system are facilitated and achieved through the web interface. In addition to providing web services, which are invoked by other remote systems, such as MSMS, DSS, PSS, etc., TrustMan system provides web-based functionalities, which can be accessed by human users through the web interface. Thus the web interface designed for TrustMan system facilitates the interactions needed by human users.

**Componential architecture for TrustMan system:** The architecture for TrustMan system, which adopts the standard definitions for web service technology for layers' classification, consists of four main layers, namely: *presentation layer, process layer, description layer, and message layer* (Fig. 8). The components of TrustMan system included in each layer are further described in the following paragraphs.

1) Presentation layer

The presentation layer, as from definition, is responsible for the delivery of information from the process layer to the web interface in a format that is readable by human being. The layer is also responsible for transforming data, which is submitted by human user to the format that is understandable and acceptable by various modules at the process layer. As such, it relieves the process layer of concerns regarding syntactical differences in data representation which is understandable by the human end-user based on the web format. Thus the presentation layer is the first and the only layer where people can care about what they are sending at an advanced level than just a bunch of ones or zeros.

TrustMan system stores, manages, and deals with sensitive information, which in most cases the VBE member organizations considers as confidential, such as strategic business data. In TrustMan system, at this layer, the web interface that facilitates the accessibility of information as well as execution of various supported services are based on the specified user rights and roles. There are three kinds of web interfaces at this layer namely: *Public, Restricted, and Protected interfaces.*

The *Public interface* provides accessibilities to information, which can be seen and read by the entire public. There is no control to such information and is

open to the public. The information that can be accessed with this interface is very limited and in fact is only advertisements and general information that are related to trust of the member, VBE administration and VBE self.

The *Restricted interface* provides accessibilities to information visible to VBE member organizations only. With this interface, member organizations can see restricted information about others, such as their current trust level but without the details on the partial results for those trust level. They can also access some strategic information, which by definition is restricted. The public cannot access information through the restricted interface.

The *Protected interface* provides accessibilities to administrative data and execution of various functionalities for assessing trust level of members in the VBE. The interface supports the VBE administrator or other organizations provided with temporary administration rights, such as VO planner, to assess trust level of member organizations within the VBE. Also, a member organization can assess its trust level. Thus with this interface, member organization can also see all the details for their own trust records in TrustMan system.

Components for public interface belong to the group of results provisional components in the operational architecture. Components for restricted and protected interfaces belong to both user control components (associated with user rights and roles) and results provision components (associated with presenting records) in the operational architecture as in Fig. 7.

2) *Process layer*

In daily life, activities are scheduled in a way that each one is known when it will be performed; following which activity, and which activity will follow soon after the preceding activity is completed. Similarly, when a service is invoked, processes that must be executed shall be organized. The process layer is responsible for defining the logic of execution for various processes (modules) to provide the requested service. The processes' scheduling constitutes of *orchestration and choreography*.

*Orchestration* refers to the sequence and flow for execution of functions within one process. For example, in java programming this refers to the order for execution of functions within one class. *Choreography* is collaborative in nature among various processes to accomplish the requested service. Thus choreography defines the logic upon which various processes will be executed or will interact through exchange of messages (parameters) to deliver the requested service.

Various development tools and languages are being used for the development of services at the process layer. Among others the popular ones are the business process execution language (BPEL), business process markup language (BPML), etc., which are based on xml programming language [25] and java web services, which are developed using java-programming language [17]. In this layer, four main components were developed to provide services related to various functionalities in TrustMan system. These components include: *Base trust level assessment*, *specific trustworthiness evaluation*, *VBE trust creation* and *TrustMan service* (Fig. 8). These

components were implemented using java. The TrustMan system is developed to run in Tomcat axis server, which supports java web services. Below we address the components of TrustMan included in this layer.

*Component for assessment of base trust level:* we refer to base trust level as the specified minimum trustworthiness that keeps an organization acceptable as a member in the VBE. This component provides services for assessing the base trust level of organizations in the VBEs. The results of the assessment from this component are accessible through the restricted and protected interfaces. However, the assessment process can be achieved via the protected interface only. For invocation, this service can be invoked via the TrustMan general service. This component constitutes two other sub-components, namely for supporting: *periodic assessment of base trust level for members* and *one-time assessment of base trust level for a member applicant* [22].

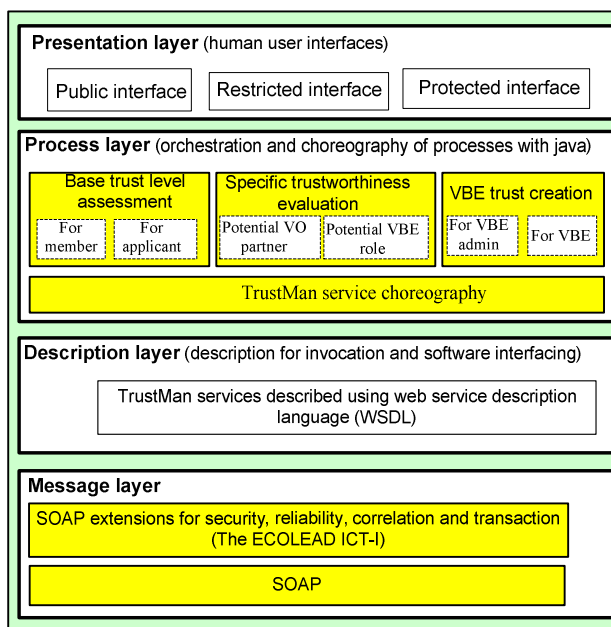


Figure 8. Componential architecture for TrustMan system.

*Component for evaluation of specific trustworthiness:* The evaluation of specific trustworthiness aims at measuring how trustworthy an organization is for a specific trust objective, such as inviting an organization to participate in a VO, appoint an organization to become a VO coordinator, choosing a VBE administrator, etc. It supports some complex operations, such as both the selection of trust criteria and the setting of the ranges for various trust levels that take place dynamically. This component provides the service for dynamic evaluation of organization's trustworthiness for specific trust objective defined by the trustor organization. The component constitutes two sub-components, namely for supporting the evaluation of specific trustworthiness for: (1) *potential VO partners* (2) *potential VBE member organizations to take VBE administrative roles*, such as VBE administrator, VO planner, etc. [22].

*Component for creating trust to the VBE:* External stakeholders must create trust to the VBE before they

make decision for various purposes, e.g. when an invited organization needs to create trust to the VBE in order to decide about accepting the invitation and thus join the VBE. Also, when a customer wants to select a trustworthier VBE to provide the business opportunity, it must also be supported. This component provides a service, which supports these external stakeholders to achieve their trust creation purposes by guiding them to access the specific suitable information.

*Component for TrustMan general service:* As stated earlier, the TrustMan system interacts with other systems through service invocation. This component was design to provide the condensed choreographic view and acts as a bridge/hub through which other specific services provided by TrustMan system can be invoked. Some java classes, (see Fig. 9) developed for this component, were used for the generation of the WSDL files as presented in the next paragraphs for description layer.

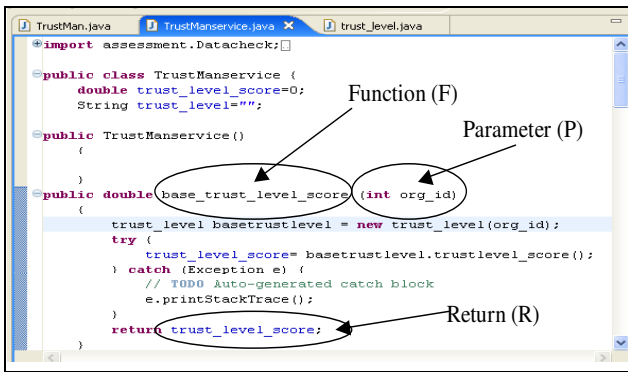


Figure 9. Part of java code for TrustMan choreograph component.

Please note the process layer constitutes the actual services that are scheduled and executed. All components in this layer belong to the group of “service components” in the operation architecture as shown in Fig. 7.

3) *Description layer*

The description layer is responsible for providing the grammatical specification of services provided at a certain point. This description is advertised and can be discovered in the UDDI (Universal Description, Discovery and Integration). From definition as applied in web service technologies the description of a service applies WSDL (web service description language) as shown in Fig. 10. WSDL describes four fundamental parts of the service. The first part is *Public interface*, which describes the public operations that are visible to external partners. The second part is *data type information for all message related to requests and responses* that describe the data types for the variables that should be passed to access the service. The third part is *binding information related to the transport protocol*, which defines the protocols necessary to access the service and to facilitate external communication. Lastly is the *address information for locating the specified service*, which describes the server location, and how it can be discovered in the UDDI.

WSDL files for java web services are generated from the respective java classes. A number of WSDL files for

services provided by TrustMan system were generated. A generic WSDL file providing an overview of all services was generated basically, for a java class which constitutes the specification of the class for *TrustMan service* (Fig. 10). This layer represents similar aspects as the service description in the operational architecture as in Fig. 7.

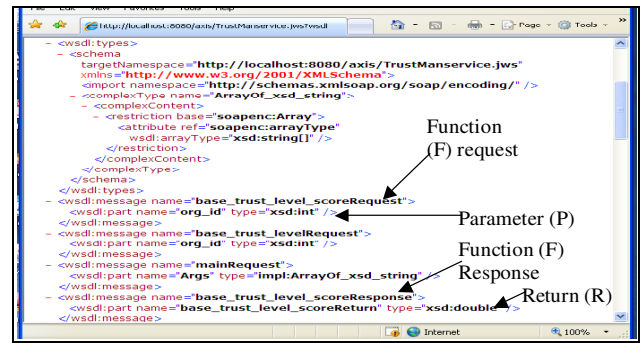


Figure 10. WSDL code for TrustMan service choreograph component.

4) *Message layer*

Until recently, web service interactions were solely synchronous and request-response in nature. However, it soon became clear that the synchronous request-response type of interaction is a very small subset of messaging scenarios. Messaging is very important in constructing loosely coupled systems, and as a result, this limitation is critical [9]. Web service specifications, such as WS-addressing and WSDL, have incorporated the concepts of messaging and lay the foundation to cover a wider range of messaging scenarios. The Tomcat Apache Axis architecture, which its implementation is applied here as web service server for TrustMan system, assumes neither one message exchange pattern nor synchronous/asynchronous behavior.

The message layer defines the protocols for communication, credential information, and sends that information across the network so that a receiving server/client can be able to interpret it. The standard communication protocol for web services is SOAP (Simple Object Access Protocol). On top of the standard SOAP protocol, addition mechanisms can be added to enhance: security, reliability, adaptability, etc. The ECOLEAD project has developed the so-called ICT infrastructure (ICT-I) (Fig. 11) for providing the necessary measures to facilitate interactions among services needed for supporting the collaborations among organizations in collaborative networks [17].

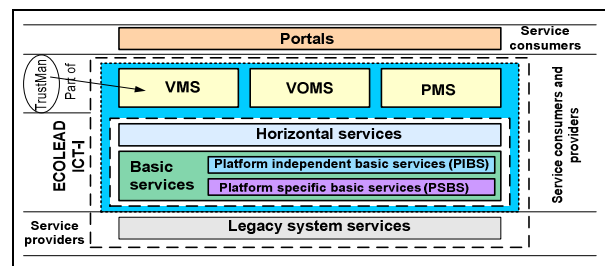


Figure 11. ECOLEAD ICT-I architecture.

The middle section of Fig. 11 shows the general architecture of the ECOLEAD ICT-I. *The TrustMan system is part of the VMS.* The VOMS (VO management system) and PMS (Professional virtual community (PVC) management system), as shown in Fig. 11, are beyond the scope of this paper but are detailed at [www.ecolead.org](http://www.ecolead.org).

VI. EXECUTION PATH FOR TRUSTMAN SYSTEM

This section addresses the design for the services' execution paths. Thus it describes the logic that the system executes several modules to provide a requested service. The section ends by providing some experimental results.

A. Services execution architecture

The implementation of the mechanisms for the execution of various components in the TrustMan system represented based on the generic execution paths for web services' is shown in Fig. 12.

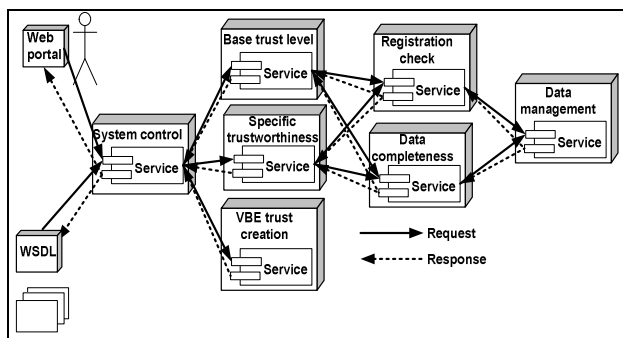


Figure 12. Overall services' execution path for TrustMan based on web service integration.

The system control component of the TrustMan system acts as the hub of interactions among other components by linking the interactions between users and the system as whole. The execution of services for human users is initiated through the web portal. The execution of services for the remote system users is initiated through WSDL files. Table IV summarizes the details of functions for each component as shown in Fig. 12.

TABLE IV. THE DESCRIPTION OF EXAMPLE SERVICES

Service	Function
System control	Controls user rights and interactions among other services
Base trust level	Assesses the base trust level of organizations
Specific trustworthiness	Assesses the specific trustworthiness of organizations
VBE trust	Provide information for enhancing trust of VBE administrator and VBE self
Registration check	Checks whether the organization is registered in the VBE
Data completeness	Checks whether the trust related data in the system is complete
Data management	Facilitates the retrieval, update and insertion of trust related data to the system data store.

B. Experimentation

The system was tried by four VBE networks, namely: IECOS (Mexico), CebeNetwork (Germany), SMT

(Switzerland) and ISOIN (Spain). Due to the confidentiality reasons for the data provided by the organizations involved in these VBE networks their actual name were replaced with assumed ones. The data applied for the trust level assessment is the organizational performance on technological, social, managerial, economical, and structural aspects. The performance data is represented in terms of trust criteria as shown in Fig. 2. Fig. 13 shows a screenshot of results for one services tested by data from IECOS. It shows the trust levels of organizations and their respective comparative scores. The lowest part of Fig. 13 shows a Trust-Meter applied for qualitatively ranking the organizations' trustworthiness based on the analysis results which applied quantitative measures. Some assumed sample organizations are indicated with their respective represented trust levels in the Trust-Meter.

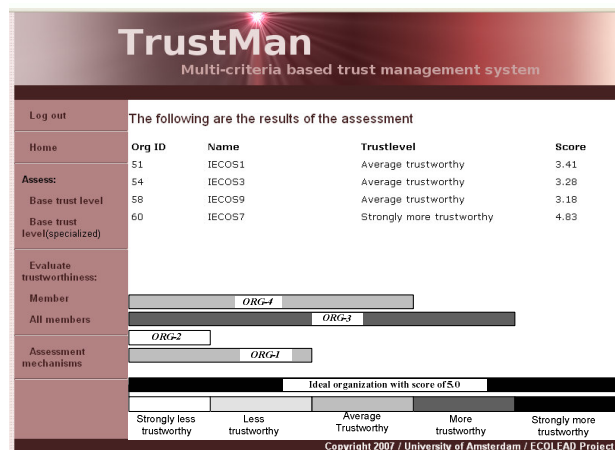


Figure 13. Screenshot for the results from assessment of base trust level of organizations.

VII. CONCLUSION

This paper has contributed to proposing an approach for the identification of trust elements for VBEs. It addresses the analysis of inter-relations and influences among the identified trust elements. It also presents general trust elements for VBE main trust objectives.

The paper has also addressed the architectural design for TrustMan system and specifically its operational and componential architectures. The services provided by TrustMan system are also described in this paper.

**Acknowledgement:** This work was supported in part by the ECOLEAD project funded by the European Commission. The authors acknowledge contributions from partners in ECOLEAD.

VIII. REFERENCES

- [1] C. Peltz, Web services orchestration and choreography. *In IEEE computer*, Vol. 36, No. 10, 2003.
- [2] C. V. D. Weth and K. Bohm, A unifying Framework for Behavior-Based Trust Models. *OTM 2006, LNCS 4275*.
- [3] D.M. Rousseau, S. B. Sitkin, R. S. Burt and C. Camerer, Not so different after all: A cross-discipline view of trust. *Academic management review*. 23, pg 393-404, 1998.

- [4] F. Niederman, and C.M. Beise, Defining the "virtualness" of groups, teams, and meetings. *Proceedings of the SIGPR Conf. on Computer Personnel Research*, 1999.
- [5] F. Ulivieri, Naive approaches to trust building in web technologies. *ISTC-Technical report*, vol. 15426B, 2004.
- [6] G. D. Fowler, and M. E. Wackerbarth, Audio teleconferencing versus face-to-face conferencing: A synthesis of the literature. *Western Journal of Speech Communication*, 44, pg. 236-252, 1980.
- [7] G.S. Ludwig, Virtual geographic research teams: A case study. *In the Journal of Geography*, Vol. 98, No. 3, pg. 149-154, 1999
- [8] H. Afsarmanesh and L. Camarinha-Matos, A framework for management of virtual organization breeding environments, *In Collaborative Networks and their Breeding Environments*, Springer, pg. 35-49, 2005.
- [9] H. Kreger, Fulfilling the web services promise. *In the Communications of ACM*, Vol 46, No. 6, 2003.
- [10] I. Mezgar, Trust building for enhancing collaboration in virtual organizations. *In Network-Centric Collaboration and Supporting Frameworks*, Camarinha-Matos, L., Afsarmanesh, H., Ollus, M.-Eds, 2006.
- [11] J.M. Seigneur, and C.D. Jensen, Trading Privacy for Trust. *In Trust Management*, LNCS, 2004.
- [12] J. Papows, The rapid evolution of collaborative tools: A paradigm shift. *Telecommunications*, 32, pp. 31-32, 1998.
- [13] L. Camarinha-Matos and H. Afsarmanesh, Collaborative Networks: Value creation in a knowledge society. *In knowledge enterprise: Intelligent strategies in product design, manufacturing and management*. Springer, 2006.
- [14] M. Castells, The rise of the network society. *The information age – Economy, society and culture*, vol. 1, Oxford:Blackwell, 1996.
- [15] N. Akkok, The causal modeling technique. *Thesis for the degree of Cand. Scient. in informatics, computer science section*, institute of informatics, university of Oslo, 1998.
- [16] R.C. Mayer, J.H. Davis, and F.D. Schoorman, An integrated model of organizational trust. *In Academic of Management review*, Vol 20 No. 3, pg 709-734, 1995.
- [17] R.J. Rabelo, S. Gusmeroli, C. Arana, and C. Nagellen, The ECOLEAD ICT infrastructure for collaborative networked organizations. *In Network-Centric Collaboration and Supporting Frameworks*, Camarinha-Matos, L., Afsarmanesh, H., Ollus, M.-Eds, pg. 161-172, 2006.
- [18] S. Greenland and B. Brumback, An overview of relations among causal modeling methods. *In the Journal of epidemiology*, 2002.
- [19] S. Jones, M. Wilikens, P. Morris and M. Masera, Trust requirements in e-business. *Communications of the ACM*, 43(12), pg 81-87, 2000.
- [20] S.S. Msanjila, and H. Afsarmanesh, Trust Analysis and Assessment in Virtual Organizations Breeding Environments. *In the International Journal of Production Research*, Taylor & Francis. ISBN 0020-7543, pg. 1-43, 2007.
- [21] S.S. Msanjila, and H. Afsarmanesh, Modelling trust relationships in collaborative networked organizations. *In the international Journal of Technology Transfer and Commercialization*, Vol. 1, issue 1, pg 40-55, 2007.
- [22] S.S. Msanjila, and H. Afsarmanesh, Specification of TrustMan system for assisting management of VBEs. *In Lecture Notes in Computer Science Series*, LNCS 4657, pg 34-43, 2007.
- [23] S.S. Msanjila, and H. Afsarmanesh, Assessment and creation of trust in VBEs. *In Network-Centric Collaboration and Supporting Frameworks*, Camarinha-Matos, L., Afsarmanesh, H., Ollus, M.-Eds, pg.161-172, 2006.
- [24] S.S. Msanjila, and H. Afsarmanesh, Understanding and modeling trust relationships in collaborative networked organizations. *In Business, Law and Technology: Present and Emerging Trends*, Vol. 2, pp 402-416, 2006.
- [25] S.S. Msanjila, T.W. Tewoldeberhan, M. Janssen, W. Block-Bockstel, and A. Verbraeck, "E-supply chain orchestration using web service technologies: A case using BPEL4WS". *In the proceedings of IRMA conference*. May 2005.
- [26] T. Grandison, and Sloman, A survey of trust in internet applications. *In IEEE communications survey and tutorials*. Fourth quarter, 2000.
- [27] T. M. Jones, and N. E. Bowie, Moral hazards on the road to the "virtual" corporation. *In Business Ethics Quarterly*, 8, 273-292, 1998.

**Mr. Simon Samwel Msanjila** has graduated BSc. in Computer Science in 2001 from the University of Dar es Salaam, Tanzania and MSc. in Systems Engineering in 2004 from Delft University of Technology, The Netherlands. Since September 2004, he has started his PhD research at the Computer Science department of the University of Amsterdam specializing on trust management for collaborative networked organizations. His current research is performed in the European project called ECOLEAD ([www.ecolead.org](http://www.ecolead.org)). He has published a number of papers in journals, book chapters and peer reviewed conferences in areas of trust management for collaborative networked organizations, web-services, and modeling and simulation of web-service based business processes.

**Dr. Hamideh Afsarmanesh** is an associate professor at the Computer Science Department of the faculty of Science of the University of Amsterdam in the Netherlands. At this faculty, she is also the director of the COL-NET (Collaborative Network) group. She has received her PhD in Computer Science from the University of Southern California (USC) in 1985, and her MSc degree also in Computer Science from the University of California, Los Angeles (UCLA) in 1980. Her current research focuses on the areas of Federated /Distributed Cooperative Databases, Virtual Organizations /Virtual Laboratories /Virtual Communities, Integration of Autonomous and Heterogeneous Databases, and the design and development of specialized Web-based Applications for a wide variety of domains such as Bio-Informatics, Manufacturing, Tele-assistance, and Distributed Control Engineering. She has directed research in more than fifteen National, European, and International projects. She has been involved in the organization and has initiated / chaired several International conferences and workshops. She has published more than 150 articles in journals, books, and refereed conference proceedings in computer science research. She has co-edited more than ten books and various issues of international Journals. She is the Dutch representative at the IFIP TC5, and a member of the IFIP WG5.3 and WG5.5.