Msanjila, Simon Samwel

Article

The insight of trust engineering for 21st century organizations

The International Journal of Management Science and Information Technology (IJMSIT)

Provided in Cooperation with:
North American Institute of Science and Information Technology (NAISIT), Toronto

Suggested Citation: Msanjila, Simon Samwel (2013) : The insight of trust engineering for 21st century organizations, The International Journal of Management Science and Information Technology (IJMSIT), ISSN 1923-0273, NAISIT Publishers, Toronto, Iss. 7-(Jan-Mar), pp. 49-75

This Version is available at:
https://hdl.handle.net/10419/97873

An official publication of The North American
Institute of Science and Information Technology

ISSN:1923-0265

INTERNATIONAL JOURNAL OF

Management Science and Information Technology

NAISIT
PUBLISHERS

www.naisit.org

The International Journal of Management Science and Information Technology (IJMSIT)

NAISIT Publishers

The International Journal of Management Science and Information Technology (IJMSIT)

NAISIT Publishers

Issue7 - (Jan-Mar 2013)

Table of Contents

This is one paper of
The International Journal of Management Science and Information Technology (IJMSIT)
Issue7 - (Jan-Mar 2013)

NAIST North American Institute of Science and Information Technology

The International Journal of Management Science and Information Technology (IJMSIT)
Issue7 - (Jan-Mar 2013) (49 - 74)

The Insight of Trust Engineering for 21st Century Organizations

Simon Samwel Msanjila
Mzumbe University, Tanzania
simon.msanjila@gmail.com

Abstract

The effective smoothening factor in different forms of collaboration has proven to be getting trustworthy partner organizations. Nowadays, trust among the 21st century organizations should be analyzed and assessed with a look from a different angle than how it has been conceptualized and addressed for such organizations in the past. In the past as it has been commonly practiced, the concept of trust has been addressed considering one chosen criterion which in most cases is subjective and not measurable. The trust analysis has also been performed at the level of one actor such as individual or organization without any comparativeness to other actors. In practice, also trustworthiness in an actor has been assumed to be a phenomenon that naturally emerges rather than being created. Furthermore, in past research, trust has been considered to be a subjective aspect and emerging from opinions and recommendations from other peers. On these bases it has been difficult to justify the rationality of trust attached to an actor for collaboration. Today the concept of trust has become an amenable factor for smoothening inter-organizational collaboration and thus has raised the need to enhance the rationality in trustworthiness measurements. Therefore, the 21st century organizations need to reconsider their working approach with incorporating trust creation and enhancement strategies. This article surveys existing work on inter-organizational trust addressing the complementary and contradictory concepts, as well as different practices in various disciplines. The article then analyzes the trust criteria and approaches for assessment of trust in organization during this 21st century.

Key words: trustworthy organizations, trustworthiness, trust, collaborative networks, new face organizations

1 Introduction

One key challenge related to both the establishment and operation of Collaborative Networks (CNs) constituting organizations as members, and in particular to short-term goal-oriented CNs, is the identification and selection of trustworthy partners for the purpose of collaboration and with the aim of fulfilling business opportunities. It is more challenging for the 21st century organizations that have been labeled as new face organizations due to their dynamic nature of their operations [Msanjila, 2012]. In contrast to the past, a new face organization (NFO) is here referred to as a rationally trustworthy firm capable of collaborating with other similar firms and can co-work in virtual collaborative networks.

Collaborative Networks (CN) emerged a few years ago, as a key issue for economic growth and a very active area of scientific production. Dynamic collaborative organizations appearing with new faces to the

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

market are an essential answer to the increasing need of strong adaptability to a constantly changing economic context [Camarinha-Matos &Afsarmanesh, 2006]. Several collaborative forms such as Virtual Organizations, Virtual Enterprises and other forms of Enterprise Networks, Professional Virtual Communities, or industry clusters and business ecosystems are now supported by large research and business practice communities [Labero, et al 2006]. These new organizational forms put forth the development of a new theoretical background. In the recent years, many international projects have contributed to these scientific advances [Camarinha-Matos &Afsamanesh, 2008]. The accumulated body of empiric knowledge and the size of the involved research community provide the basis for the foundation of a new scientific discipline on "Collaborative Networks" (Afsarmanesh et al., 2007). Thus the discipline of collaborative network is strongly multidisciplinary with mixed contributions from Engineering, Economics, Managerial, Socio-Human communities, etc.

Collaboration among these NFOs appears essential to achieve Sustainable Development. Sustainability requires conceiving new forms of collaboration at every level of the market. New areas and patterns of collaborative behaviors are emerging, not only in industry, but also in the services sector, as well as in governmental and non-governmental organizations. Fundamentals of Collaborative Networks such as proper theoretical principles, management of collaboration risks and benefits, new value systems, adequate performance assessment methods, or trust establishment approaches, still represent important research challenges in formulating a sound theory for building inter-organizational collaboration. This paper proposes steps and approaches for creating new face organizations.

For the remaining part of this paper is organized as follows: in Section 2 we present the key concepts of trust as applied for organizations; Section 3 presents the benefits and the need for inter-organizational trust in collaborative environment; section 4 for addresses the factors and indicators that need to be considered when an organization want to enhance its trustworthiness against others for collaboration purposes; section 5 presents the steps that an organization is recommended to follow when trying to establish its trust in a network environment; section 6 presents the challenges related to inter-organizational trust that are in need for further research; and lastly section 7 concludes the paper.

2 Key concepts of trustworthy organizations

Due to the variations in trust interpretation and the variations in trust perception in both practice and research, the concept of trust is defined differently in various disciplines. Consequently, trust has proven to be a complex aspectwhich is influenced by indicators originating fromdifferent disciplines. Some actors have been assuming to be related to some of the following indicators: security, risks, privacy, belief, honesty, truthfulness, competency, reliability, past history, and so on. Until today, there is still no consensus in the literature on what trust means and what constitutes the management of trust between different entities, such as individuals or organizations (Povey, 1999). The lack of consensus on the definition of trust has led researchers to define trust differently for the purposes of providing a common understanding in their specific domain or application environment.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

With respect to online transaction technology, Kini and Choobineh (1998) have addressed the theoretical framework of online trust, examining it from the perspective of personality theorists, sociologists, economists, and psychologists. In their work they started by defining trust according to the Webster dictionary as: *an assumed reliance on a person or something. It is a confident dependence on the character, ability, strength, or truth of someone or something. It is a charge / duty imposed in faith / confidence or as a condition of a relationship. Thus it simply means to place confidence in an entity.*

The European Commission Joint Research Center defined trust *as "the property of a business relationship such that reliance can be placed on the business partner and the business transactions developed with them"* (Jones, et al., 2000). This view of trust is based on the area of business management and provides an interesting analysis of what must be done to enable and enhance trust between partners in business. In the analysis related to her work, Jones (Jones et al., 2000) stated that the following aspects of trust are fundamental for partners in business:

- The identification and reliability of business partners.
- The confidentiality, availability, integrity and risks on sensitive information.
- The prevention of unauthorized copying and use of information.
- The guaranteed quality of products and services.
- The dependability of computer services and systems (availability, reliability, and integrity of infrastructure; the guaranteed level of services; and management of risks on infrastructure).

The Oxford Dictionary defines trust as *the firm belief in the reliability, truth or strength of an entity*. In this definition, a trustworthy entity is basically highly reliable and so will not fail during the course of an interaction; will provide a service or perform an action within a reasonable period of time; will tell the truth and remain honest with respect to interactions; and will not disclose confidential information.

In view of these varied definitions, trust can be regarded as a composition of many different attributes: reliability, dependability, honesty, truthfulness, security, competency, past history of individuals, timelines, and so forth. Any of these may be considered, depending on the environment and application for which the trust is being specified. Other popular definitions dominating research on trust in different entities are:

- *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 (Mayer, et al., 1995).*
- *Trust is the belief in the competency of an entity to act dependably, securely and reliably within a specified context (Grandison&Sloman, 2000).*
- *Trust is a psychological condition comprising the trustor's intention to accept vulnerability based upon positive expectation of trustee's intentions and behavior (Rousseau, et al., 1998).*

In spite of the attempts to define trust in research, as discussed in section 4, and the difficulty to reach consensus among researchers, the word "trust" in relation to inter-personal trust in particular and as

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

used daily by individuals refers to one person's opinion of another person. Not only is an estimation of another's intention needed to establish inter-personal trust relationships, but also an estimation of others' potential competencies. Therefore, while this work can benefit from general past research on trust relationships between actors, the results of such research cannot be directly applied. Trust between new face organizations to support collaboration is a more complex subject, which must be addressed in relation to the interdisciplinary between the domains and the heterogeneities and contradictions between the interests and the goals of organizations involved. Some crucial research areas might include the *identification and tuning of trust elements, modeling of trust and trust elements, assessment of trust level,* andthe *establishment and promotion of trust relationship*which constitute the main focus of the management of trust among new face organizations. The following definition of trust between two organizations:

> *Trust between two organizations is the objective-specific confidence of a trustor organization to a trustee organization based on the results of rational (fact-based) assessment of the trustee organization's level of trust (Msanjila&Afsarmanesh, 2007).*

In relation to trust of NFO which aims at co-working with others in a specific collaborative opportunity the following important terms represents the basic concepts and their respective definitions(Msanjila, 2009):

- *Trust between NFOs* is the objective-specific confidence of a trustorNFO to a trustee NFO based on the results of rational (fact-based) assessment of the trustee NFO's level of trust.
- *Trust actors*: refer to the two NFO parties involved in a specific trust relationship. The first party is the NFO that needs to assess the trustworthiness of another, and is referred to as the trustor NFO. The second party is the NFO that needs to be trusted and which will thus have its level of trust assessed; and it is referred to as the trustee NFO.
- *Trust level*: refers to the level of intensity of trust for a trustee NFO in a trust relationship, based on an assessment of the values for a set of necessary trust criteria. Clearly enough, the criteria for assessment of NFO's level of trust vary and have a wide spectrum, depending on the specific purpose (e.g. the requirements, the perspective, and the objective of the establishment of trust). When the level of trust is assessed for a specific purpose the assessment is based on specific trust criteria for that specific purpose, the evaluated trust level results are referred to as the specific trustworthiness of that NFO.
- *Trust level assessment*: refers to the examination of the trustworthiness of the NFO using certain defined indicators. Many approaches are used to assess different entities' level of trust. In our previous work we have proposed a multi-criteria approach for analyzing the trust in organizations (Msanjila&Afsarmanesh, 2008). Based on this approach, rational mechanisms have been developed to assess the level of trust in organizations.
- *Trust relationship*: a relationship is a state of connectedness between people or organizations, or a state involving mutual dealing between people or parties. Here, trust relationship refers to the state of connectedness between a trustorNFO and a trustee NFO whose intensity is characterized and based on the trust level.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

3 Benefits and importance of trustworthy organizations

In order for a NFO to effectively participate in a collaborative networks and thoroughly gain the benefits, at the base of its preparation stage are the adoption of the common ICT infrastructure and the interoperability approach, which together constitute the minimum base for any cooperation/collaboration network. By managing to establish itself as a trustworthy NFO and thus facilitate its collaboration with other NFOs the organization shall be able to gain the following:

- Share business processes: Trustworthy NFO shall gain the possibility of participating in initiated business processes organized by other NFOs and thus enhance its business efficiency. It will thus have the chance to exercise different sets of processes, standards and practices, and a different level of autonomy with other NFOs. Depending on the level of cooperation required although this is obvious benefits but it might prove challenging and complex for untrustworthy firms.
- Share scarce business resources: Trustworthy NFOs need to possess business resources that are valuable to an established collaboration. However, business opportunities are increasingly becoming complex in terms of too large demanded amount of business resources for each individual NFO to equip. Due to its trustworthiness and willingness to collaborate the NFO shall have a chance to complement its missing resources through sharing such scarce resources with other NFOs. In addition to willingness, in order for a NFO to share resources with others, this requirement implies compliance with the common sharing policies, and the need for experience, skill, knowledge, and so on to prepare the sharable objects, and to support this sharing activity. For example, in order to prepare to share a technology-related resource (such as computation facilities), the organization must make sure that the resources comply with some standards in a CN, such as those relating to communication and interoperability.
- Share scarce business competencies: It is difficult for a NFO to acquire all the competencies that are necessary to assure its existence in business and thus get competitive opportunities. In collaborative networks, there is a chance to share competencies of other organizations and the proper management of these available and emerging competencies in CNs is the necessary base element to support this requirement. These NFOs must be prepared to offer some of their own competencies for this purpose, as well as benefit from the pool of available competencies in the CNs.

A catalyst for the enhancement of cooperation between NFOs is the establishment of trust relationships, which is why past research states that trust is the most salient factor for cooperation networks in achieving the network objectives (Morgan & Hunt, 1994). Trust relationships between NFOs are more important for large collaborative networks where direct personal contact are more difficult to achieve by all, while they shall operate under pressure from the global economy, the increasing value of information, and the mounting uncertainties surrounding their businesses (Msanjila&Afsarmanesh, 2008). Several advantages can be gained once trust relationships between NFOs have been properly established and managed trust relationships including:

- Facilitating the achievement of common goals through information exchange, knowledge sharing, tools sharing, and so forth, between member organizations.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

- Enabling the member organizations to cope with uncertain or incomplete information.
- Easing the process of creating and launching consortiums and smoothing the partner selection processes.
- Accelerating the contract negotiation process between selected partners for the consortium.
- Encouraging the member organizations to avoid opportunistic behaviour during collaboration.
- Achieving the competitive advantage, through reduction of governance internalization (acquisitions) tasks, and thus the transaction costs.
- Enabling open communication and thus reducing conflicts between member organizations.

4 Critical success factors for trustworthy organizations

The management of collaborative networks particularly related to the establishment of inter-organizational trust relationships differ widely from the management of traditional organizations. In principle, management of traditional firms comprises directing and controlling a group of people or entities (e.g. departments, or organizations) for the purpose of coordinating and harmonizing that group towards accomplishing a common goal (Howe, 2004). In traditional practices, management often encompasses the deployment and manipulation of human resources, financial resources, technological resources, and natural resources in a company. However, it can also refer to the individual or a group of people who perform the act(s) of management. The generic categories of management include (Center, 2008).

- Organizing: making optimum use of the existing resources to enable the successful implementation of plans.
- Controlling/monitoring: checking progress against plans, which may need plan modification according to feedbacks.
- Planning: deciding what needs to be performed in future, e.g. immediately or in weeks, months, years, etc.), and generating plans of action to reach the objectives.
- Leading/Motivating: applying mechanisms and strategies to get others into playing an effective part in achieving plans.

The above definitions have been applied successfully to the management of traditional organizations with static structures, such as traditional business companies. These organizations typically practice repetitive and fixed business processes. The following fundamental aspects indicate the static nature of traditional organizational structures [Msanjila&Afsarmanesh, 2007a]:

- *Fixed or known resources*: products or services that a traditional organization can offer to its customers are usually well defined and standardized. These products or services can only be customized to meet specific customer requirements, but usually they do not require re-development. Thus, the resources that are needed for manufacturing products or providing services are usually known before a specific opportunity is acquired. These resources can be obtained and kept in an organization a priori to the search for and the acquisition of business opportunities. The management of resources mostly focuses on either ensuring their availability within an organization or on time acquisition whenever is needed.
- *Fixed or known competencies*: as stated above, products or services that a traditional organization can offer are usually known and standardized. Thus, the competencies that are required to support the manufacture of products or the provision of services are also known and

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

standardized. The management of such competencies is mainly focused on either enhancing the existing ones (e.g. through specialized training of employee) or acquiring new or qualified employees.

- *Static and specific business strategies*: products or services that can be offered by traditional organizations are usually standardized. Therefore, these organizations maintain static or long-term business strategies. These strategies focus on, for example, keeping past customers for as long as possible, or acquiring as many new customers as possible. The management of these processes follows well-defined organizational business strategies.
- *Static sharing and operating principles*: most traditional organizations have a culture of sharing achievements (e.g. percentage of yearly profit) with their employees, which may be offered as a motivation benefit (e.g. end of year bonus). The principles used to distribute such benefits are usually known and standard within an organization and depend on aspects such as salary levels, employee positions and employee performances. The management of these activities therefore, follows defined principles within the organization.

On the other hand, unlike the traditional organizational structures, NFOs in a collaborative environment are so dynamic and thus has dynamic structure and the established business processes are unique and changes for every opportunity which is acquired. For example, the creation of short term consortium is unique to each configured network since it responds to a specific opportunity. Among others, the following fundamental aspects indicate the dynamic nature and characteristics of the structures of collaborative networks which the NFO must be prepared to meet [Msanjila, 2009].

- *Dynamic resources*: Collaborative networks offer their products or services to their customers only through the configuration of short term consortiums. The resources that are required to manufacture products or provide services belong to NFO members. Therefore, these consortiums are uniquely configured constituting “best-fit” NFOs that are capable of sharing or exchanging their resources in order to respond to opportunities. The partners may change for every consortium that is configured, even if the same product or service has to be provided to a customer. Therefore, the availability of the resources cannot be known or guaranteed a priori to configuring the temporary consortiums. To succeed a NFO must be capable of operating in the environment which demands such dynamic resources.
- *Changing competencies*: The competencies of a collaborative network constitute a set of the aggregated competencies of its member NFOs. Thus, collaborative networks do not have competencies of their own beyond those of their member NFOs. The management of competencies focuses on ensuring that all of the related competencies that are needed in the market exist within the collaborative network. One fundamental approach to fill competency gaps is through inviting external organizations to become members and thus provide missing competencies. A critical factor here is the ability of the NFO to match its competencies with the changing competencies of other NFOs and thus be able to collaborate.
- *Dynamic business strategy*:Business strategies of collaborative networks need to change depending on the market changes, i.e. with a consideration for the following areas of focus: the acquisition of potential member organizations, support for opportunity brokerage, the facilitation of consortium configuration, the provision of information to actors in a network for the purpose of making informed decisions, and so forth. The critical factor in relation to this aspect is that the NFO must be prepared to make informed decision in an environment whose operational strategies are continuous changing. Thus the organization must be capable of making potential predictions.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

In addition to the new management style, in order for the NFOs to become trustworthy and ease the process of establishing trustworthiness, they must properly take into account the antecedents of trust between organizations. Trust antecedents are cardinal elements that may have a positive or negative impact on the effectiveness of the established trust relationships among organizations. Three trust antecedents are identified for NFOs in this work, namely the *shared values, the previous interactions,* and *the practiced behaviors*.

Shared values: Shared system of values occur when the trustor NFO and the trustee NFO have a common understanding on important issues that might influence the creation of trust towards each other, such as their missions, goals, policies and interpretations of right or wrong [Morgan &Hunt, 1994]. Shared values can range from business objectives to internal management processes and approaches. In business environments, it is more difficult to have shared values between two competing NFOs than between two NFOs that are complementing each other (Clay &Strauss, 2000). Typically, when two organizations have a common understanding/perception and/or belief in a set of values they both feel secure in the knowledge that there will be no unexpected results during their cooperation/collaboration. It is therefore easier to establish a trust relationship under such conditions. As an aspect of preparedness, the CN must ensure that member organizations establish shared values with other organizations.

Previous (fruitful) interactions: Previous (fruitful) interactionsbetweenthe trustor NFO and the trustee NFO - either directly or indirectly (through other intermediate organizations) – may enhance the effectiveness of established trust relationships. These time-related interactions can be formal such as the formal exchange of information, knowledge or expertise. Interactions can also involve individuals who work within the two organizations either technical or social. Even though sometimes there may be no current business-oriented interactions, yet the existence of previous informal interactions may smoothen the establishment of trust relationship among organizations. Member NFOs of the CN have the possibility and are encouraged to interact with each other.

Practiced ethical and/or moral behaviors: Practiced ethical and/or moral behaviors basically refer to the opposite of *opportunistic behavior*.Opportunistic behavior means taking immediate advantage - unethically - of any circumstance that may generate possible benefit. Traditionally, opportunistic behavior in competitive markets seemed natural because the typical focus of organizations in such environments was on the acquisition of customers, without regard for long-term relationships with other organizations. In collaborative networks however, organizations must rather cooperate in order to best serve the same customers. Opportunistic behavior has therefore a negative impact on the effectiveness of trust relationships among organizations. It mainly derives from transaction cost literature and is defined as *seeking self-interest with guile* (Mukherjee, 2003). Here we refer to opportunistic behavior as an *ungentle action that might be taken by organizations for the purpose of benefiting themselves unethically, more than others (e.g. quitting the collaboration once they have made a large gain, or when they expect the risks of the collaboration to become a threat)*.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

5 Steps towards creating a trustworthy organization

Trust in a NFO cannot be created in a short time. As stated in literature, trust takes time to be created and while being created might be evolving which means increasing and decreasing with time. The proposed steps here represents phases that can be taken to ensure that the collaborating partners are all trustworthy and thus meet the definition of new face organizations as provided in section 1. We propose four steps towards creating a trustworthy organization, namely, (1) creating trustworthy collaborative environment, (2) Enhancing understanding of trust concepts among involved firms, (3) assessing trustworthiness of potential members and (4) presenting results of assessment of trustworthiness of organizations.

STEP 1: CREATING TRUSTWORTHY COLLABORATIVE ENVIRONMENTS

Certain previous studies have assumed that the most suitable partners for establishing a new temporary consortiums may easily be identified and selected from the open universe of available organizations, for example through the Internet, and merged into the required consortium. But, this assumption overlooks a large number of obstacles in this process, among which the following can be mentioned [Afsarmanesh&Camarinha-Matos, 2005].

- How to learn of the mere existence of potential partners in the open universe and deal with incompatible sources of information.
- How to acquire basic profile information about organizations, when no common template or standard format exists.
- How to quickly establish an inter-operable collaboration infrastructure, given the heterogeneity of organizations at multi-levels, and the diversity of their systems.
- *How to build trust between organizations, which is the base for any collaboration*.
- How to develop and agree on the common principles of sharing and working together.
- How to quickly define the agreements on the roles and responsibilities of each partner in order to reflect the sharing of tasks, the rights on the produced results, and so on.

A main aim of the long-term collaborative environment, as shown in Figure 1, is focused on the transition from point-to-point connections between traditional organizations to a network structure in order to increase the chances of its member organizations' involvement in opportunities for collaboration, and to reduce the costs and time needed to configure opportunity-oriented temporary consortiums (Figure 1).

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

To conclude, the transition from point-to-point connection to networked structure enhances organizations' preparedness in the following aspects:

- Maintaining common sharing and operating principles.
- Acquiring an interoperable infrastructure.
- Achieving the same level of understanding through common ontology.
- Defining common value systems and performance metrics.
- *Creating trust between organizations.*
- Acquiring systems for assisting the management of cooperation and collaboration.

The collaborative environment need to be trustworthy by itself and trust must be created and maintained in order to enhance the interests and loyalty of the member NFOs with respect to the network establishment, a trust which in turn also increases its active involvement in temporary consortiums activities. We have identified four trust elements that together represent the primary aspects of establishing a trustworthy collaborative network for that facilitates the creation of trustworthy NFOs. These elements are related to: (1) collaborative network policies, (2) transparency and fairness in the network, (3) collaborative network branding and coverage and (4) components constituting the collaborative network.

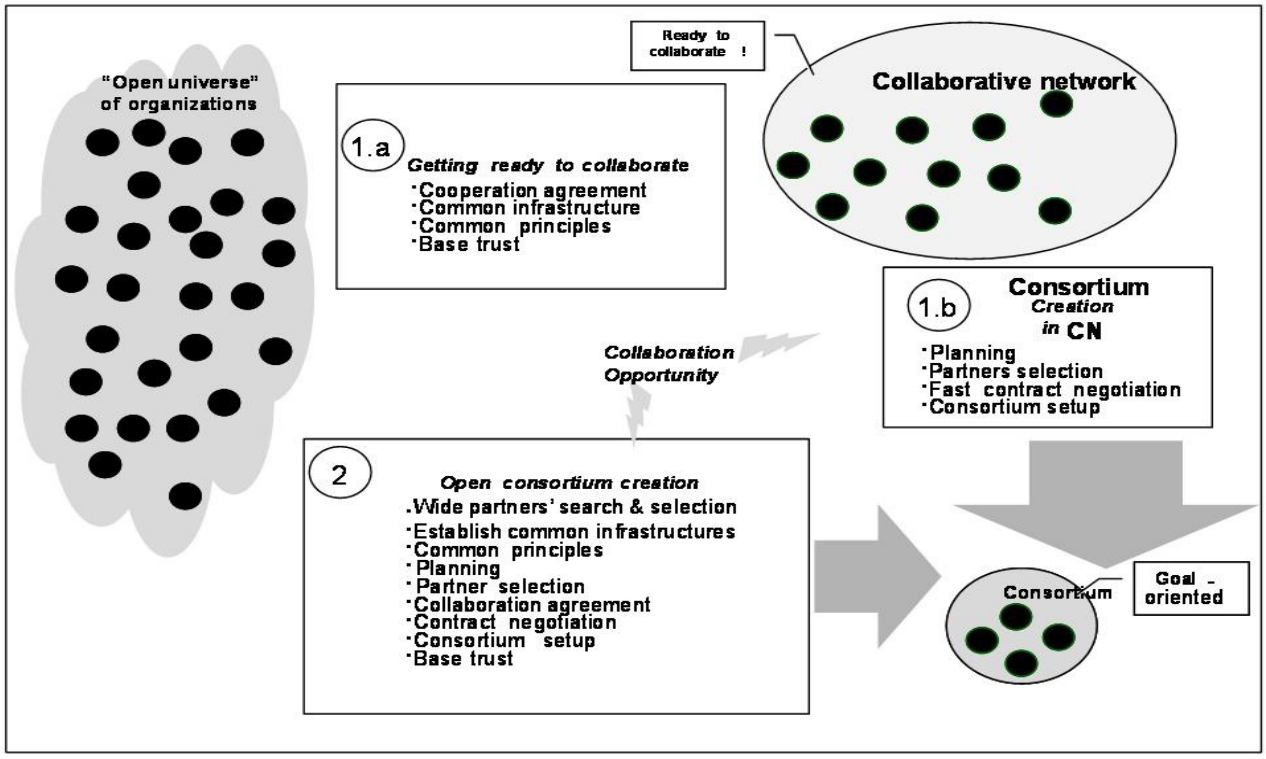

Figure 1: The visualization of a long-term collaborative network(Afsarmanesh&Camarinha-Matos, 2005)

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

Furthermore, a NFO members needs to be convinced that the network administration is trustworthy in order to join and remain active in the collaborative network. For example, since NFO members continuously compete to win an opportunity to participate in temporary consortiums that are configured within the collaborative network, they must be convinced that the administration is impartial and that the selected partners for each consortium are chosen on the basis of their qualifications.

STEP 2: ENHANCING UNDERSTANDING OF TRUST CONCEPTS

To accept and apply the results of trustworthiness assessment the organizations in a collaborative network must understand properly the concepts of trust in a collaborative environments. Some crucial concepts may include:

- Difference between inter-organizational trust and inter-personal trust
- Different practices of trust in various disciplines
- Main concepts related to trust such as risks, security, privacy and reputation
- Understanding trust elements and trust criteria for assessing trustworthiness

Trustworthy organizations vs trustworthy individuals

Many researchers have indicated that trust is an important issue in smoothening inter-personal and inter-organizational relationships. However, past research work conducted to address inter-organizational trust has focused on theoretical evaluations (Currall& Judge, 1995). Nevertheless, in the current information society some studies have addressed trust from a practical standpoint and have produced fundamental empirical evidence on the creation of trust among actors (Smith & Barclay, 1997). Even so, until today there is still no actual agreement on the exact nature and definition of the trust with respect to its conceptualization, perception, preference and measurement. To address trust in research satisfactorily, understand the effects of trust in different types of partnerships, and enable acceptable results for all stakeholders, it requires the involvement of communities and other institutions from heterogeneous domains (Smith & Barclay, 1997).

A fundamental difference between inter-personal trust and inter-organizational trust relate to their antecedents (Msanjila&Afsarmanesh, 2007d). Inter-personal trust is defined at the level of the individual and it represents the extent to which a person places trust in another person. It has been observed that although inter-organizational trust and inter-personal trust differ in a number of aspects, they share the aspects of time in relation to the *temporary and dynamic nature of trust* (Ratnasingam, 2003). For example, *time* can influence the decision on the trust related data, considering aspects such as validity, sources and mechanisms applied for its collection, which are needed to create trust among actors. Thus, time is a key aspect to consider when analyzing and modeling trust relationships among organizations.

A basic or essential level of trust is required for smoothening inter-organizational collaboration. An established climate of trust that is internalized in organizational behavior and supported by mutual belief is necessary for collaborative efforts between partner organizations (Cosimano, 2004). Optimal

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

gains from a network can be achieved through collaboration that is facilitated by inter-organizational trust, such as reduced costs, greater achievement speed, and an improved ability to handle complexity of different activities. Furthermore, trust influences an organization's long-term strategic plans, collaborative market performance and loyalty. Trust also broadly influences organizational relationships, commitment, cooperation, functional conflict, uncertainty, the propensity to leave, and acquiescence (Msanjila&Afsarmanesh, 2008a).

The difficulty in the conceptualization of trust among organizations is extending a phenomenon that is inherently at an individual level, to an organizational level. These difficulties can produce confusion in relation to the creation of inter-organizational trust.

Trust practices in different disciplines

The new face organizations collaborate to perform business processes that might be originating from different disciplines. In same line, trust is a key concept addressed by research in many disciplines and it is gaining importance in supporting collaboration among actors in the emerging information society. In this sub-section we present the reported research on perceptions of trust in five different disciplines, namely sociology, economics, psychology, politics and computer science.

In sociology, trust is defined through reputation and previous interactions among individuals. Furthermore, the ways and reasons by which reputation for trustworthiness is established or destroyed are being studied in social trust relationships. Not only will the perceivers of reputation have access to information which the reputation holder does not control, but also the manner in which both types of information are interpreted is not straightforward (Good, 1988). Therefore, individuals wish to have complete information about the people with whom they deal before dealing with them (Dasgupta, 1988).

In economics, decisions about trust are similar to decisions about taking risky choices. Individuals are assumed to be motivated to establish trust relationship with each other in order to either maximize the expected gains, or minimize the expected losses from their transactions (Josang& Lo Presti, 2004). The critical factor with respect to trust in economic studies is the risk management related to trust relationships. Trust in psychology is related to beliefs. A trusting behaviour occurs when an individual believes that there is an ambiguous path; the result of which could be good or bad (Morgan & Hunt, 1994). The occurrence of the good or bad result is contingent on the actions of another person. If the individual chooses to go down that path, he makes a trusting choice.

In politics and digital governments, trust is related to truth telling. It is important for digital government, to maintain high standards of truth telling and to avoid being associated with poor reputation and thus loosing the trust of the public (Sztompka, 1999). Trust in governments and politics is essential in order for the governments and the related political parties to remain in power. However, several other factors

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

are also identified as influential on the level of trust governments have towards their citizens, such as reputation, performance, accountability, commitment, and so on (Sztompka, 1999).

In computer science, trust has been mainly associated with security, privacy and reputation. Establishing trust among interacting systems that are developed based on the service oriented architecture depends on their compliance to the set of communication policies. These policies provide regulations that must be met by a system to be trusted (Blaze, et al., 2009). Generally, when an environment is secure, it is easier to establish trust relationships among the systems' users, and equally if a user respects the privacy of others in relation to their personal data and sensible information he can be regarded as trustworthy (Seigneur & Jensen, 2004). Reputation is being used for managing trust in systems that are developed using multi-agent technology; therefore, in multi-agent systems the trustworthiness of a trustee represented by an agent "*b*" is assessed by a trustor represented by an agent "*a*", using the reputations witnessed by the trustor (or trustor's friends) or certified by the trustee's friends (Huynh, et al., 2004).

Main concepts related to inter-organizational trust

Trust is related to different concepts and these relations either complement (such as trust and security, reputation, co-working) or contradict (such as trust versus risks, privacy, and so on.) its perceptions among actors as addressed below:

a) *Trust versus risks*

Risk is a concept that denotes a potential negative impact to an asset or some characteristics of a value that may arise from present processes or future events. In everyday usage, "risk" is often used synonymously with the probability of a known loss. Many definitions of risk depend on a specific application and situational contexts. Frequently, risk is considered as an indicator of threat. It can be assessed qualitatively or quantitatively. Qualitatively, risk is considered proportional to the expected losses which can be caused by an event and to the probability of the same event. The harsher the loss and the more likely the event, the greater the overall risk. Measuring risk is often difficult; the probability is assessed by the frequency of past similar events, which in fact is difficult to link to the future. Trust and risk are negatively related. When there is a high chance that certain risks may arise in a certain environment it is very difficult for an organization to trust other organizations in that specific environment. Moreover, when organizations trust each other they tend to relax and rely on one another based on the assumption that risks may not arise. However, this attitude may in time increase the chance of risks arising due to new changes inside each organization.

b) *Trust and security*

Inter-play between trust and security can be examined from different aspects. The two most popular aspects are: in respect to management systems and in respect to technologies owned by organizations.

Trust and security for management systems: Until a few years ago, enhancing the security of systems that are used for the management of information, resources, stored knowledge, available skills, and so forth, was the fundamental approach used to enhance trust among collaborating organizations. Since this time and even currently, the situation has changed dramatically. New security regulations, significant security, privacy incidents, and so on, are no longer enough to guarantee smooth operations for business organizations on markets that currently present continuously increasing turbulent conditions (Grandson &Sloman, 2000). Consequently, it is now fundamental that the search for solutions

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

and a balance between trust and security in relation to the ICT systems and the facilitated businesses now involves both business organizations and ICT industries.

The security of an ICT system alone is not sufficient for smoothing collaboration among organizations, and thus guaranteeing the necessary success and survival. As a result, security boundaries among organizations are fast becoming increasingly less stringent. Therefore, trust propagation that is based on the security of an ICT system is decreasing and becoming rationally specific. Applications that used to run on dedicated servers now are running on virtual environments, sharing infrastructure with others, and using widely-distributed physical resources (Rabelo, et al., 2006). This makes the process of creating inter-organizational trust with the application of system security even more difficult.

As a result of amplification of problems related to the security of ICT systems, risks associated with businesses supported with ICT systems, market turbulences, and so forth, certain other approaches for smoothing co-working environments are needed and must be considered. Managing trust among organizations, by applying rational mechanisms for assessing level of trust and creating trust, has emerged as a promising approach for achievement of the required smoothening (Msanjila&Afsarmanesh, 2007a). In our approach, systems (Trust Management systems) are suggested as a means to support organizations in the performance of tasks related to analysis and creating trust of their organization in others. A number of processes also need to be supported with tools in order to provide the required services for the management of trust among organizations.

Trust and security in relation to owned and experienced technologies: There has been a misconception about trust and security, and roles that technology plays in this binomial for setting/facilitating collaboration. Most people tend to believe that trust is merely the result of security - when security exists, actors can trust each other - but researchers have observed that this notion does not represent the entire picture (Rousseau, et al., 1998). Trust is a wider concept and its link with security is not linear (Msanjila&Afsarmanesh, 2007c). Technology can effectively provide security; for example, every step of an online transaction has one or more procedures for transmitting users' data safely, such as using cryptography and protocols technologies. However, this does not represent trust. Security-driven approaches for creating trust among organizations have led to a bias entitled "*the double illusion of 100% safe*" (Weth&Bohm, 2006).

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 occurs in both the positive area of security protocols and the negative area of hacking processes. Organizations that use security of environments that are enhanced by technology as the only means of trusting others might face difficultly when unexpected problems occur, such as the hacking of software (Grandison&Sloman, 2000). This is the first illusion.

Imagine for a moment that a secure environment has been obtained. Organizations are able to 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 that certain risks may increase (Rousseau, et al., 1998). An environment depicted with hard technology protection

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

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

c) *Trust versus privacy*

At the individual level, privacy can be seen as a fundamental human right. Similarly, organizations are now facing problems related to privacy and, more specifically, with respect to confidential data and strategies. Different legislative and technological mechanisms have been proposed to enhance the privacy of organizational data in the world of computers. Protection depends on whether privacy is seen as a right, which should be protected by laws; or a need, which should be supported by devices (Msanjila&Afsarmanesh, 2007c). From the point of view of privacy and considering the co-working among organizations, there is an inherent conflict between trust and privacy: the more knowledge a first entity gains about a second entity, the more accurate the results will be of the level of trust assessment. Nevertheless, the more knowledge is gained about the second entity, the less privacy is left to this entity (Seigneur & Jensen, 2004). The contradiction of enhancing level of trust in organizations, while at the same time enhancing their privacy, is a challenge for further research.

d) *Trust and reputation*

Reputation concerns general opinions (more technically, a social evaluation) of the public toward a person, a group of people, or an organization. It is an important factor in many domains, such as business, online communities or social status. Reputation is known to be a ubiquitous, spontaneous and highly efficient mechanism of social control in natural societies. It is a subject which is being studied in disciplines such as social, management and technological sciences. Furthermore, reputation acts on different levels of agency, namely individual and supra-individual. At the supra-individual level, it focuses on groups, communities, collectives and abstract social entities (such as firms, corporations, organizations, countries, cultures and even civilizations) and it affects phenomena at different scales, from everyday life to relationships between nations. There are two kinds of reputation: *witnessed reputation* and *certified reputation.*

Witnessed reputation(Huynh, et al., 2004) refers to the reputation-related information that is collected by the trustor, or the trustor's associated organizations (friends). In this case, the trustor organization or its associated organizations observe characters of the trustee organization to decide its trust level. In CNs, where organizations collaborate virtually, the adaptation of this approach is hardly feasible.

Certified reputation(Huynh, et al., 2004) refers to the reputation-related information that is collected by the trustee organizations and made available to the trustor organization. The trustee organization can provide information such as a detailed organization profile, recommendation letters, accreditation documents, auditing results, etc., to the trustor organization in order to enhance its trust level. The trustee organization can also request its friend/authorized organizations to provide positive information (e.g. accreditation document) to the trustor organization in order to enhance its trust level. The main problem of this approach is that there is high risk of user-biased information, which endangers the success of the resulting trust relationships. The validation of such information is also difficult since, in practice, bad reputations are usually hidden.

Understanding trust elements and trust criteria for assessing trustworthiness

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

There are *five potential trust perspectives* (Msanjila&Afsarmanesh, 2008) that a trustor NFO can assume, or choose from, for representing its "primary aspects" as a means to assess the level of trust in a trustee NFO. These perspectives constitute the so-called "*trust perspective pentagon*" as shown in Figure 2. When a NFO needs to trust another NFO, five trust perspectives to be measured may be of interest or concern to the trustor NFO, with the base assumption of their independence these perspectives include: Structural (STP), Economical (ECP), Technological (TEP), Managerial (MGP), and Social (SOP).

The assessment of level of trust in an organization occurs in three different cases. Firstly (case 1), for each membership applicant of a collaborative network, its *"base" trust level* needs to be assessed in order to be accepted as a member of the CN. The base trust level is the minimum threshold value of trust level, which allows a member organization to keep operating in the collaborative network. Secondly (case 2), periodic assessment of the base trust level for all NFO members is necessary, in order to control and preserve the trust balance at an acceptable level within the collaborative network. Tertiary (case 3) is when *specific trustworthiness* evaluation is requested by a trustor for certain "specific" purpose, such as for inviting a NFO to participate in a temporary consortium, or for appointing an organization to become consortium coordinator, and so on. In such cases the trustworthiness of the organization must be assessed for that specific purpose (Msanjila&Afsarmanesh, 2007a). Figure 2 shows a set of trust elements that can be selected for the assessment of trustworthiness of organizations in a collaborative network.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

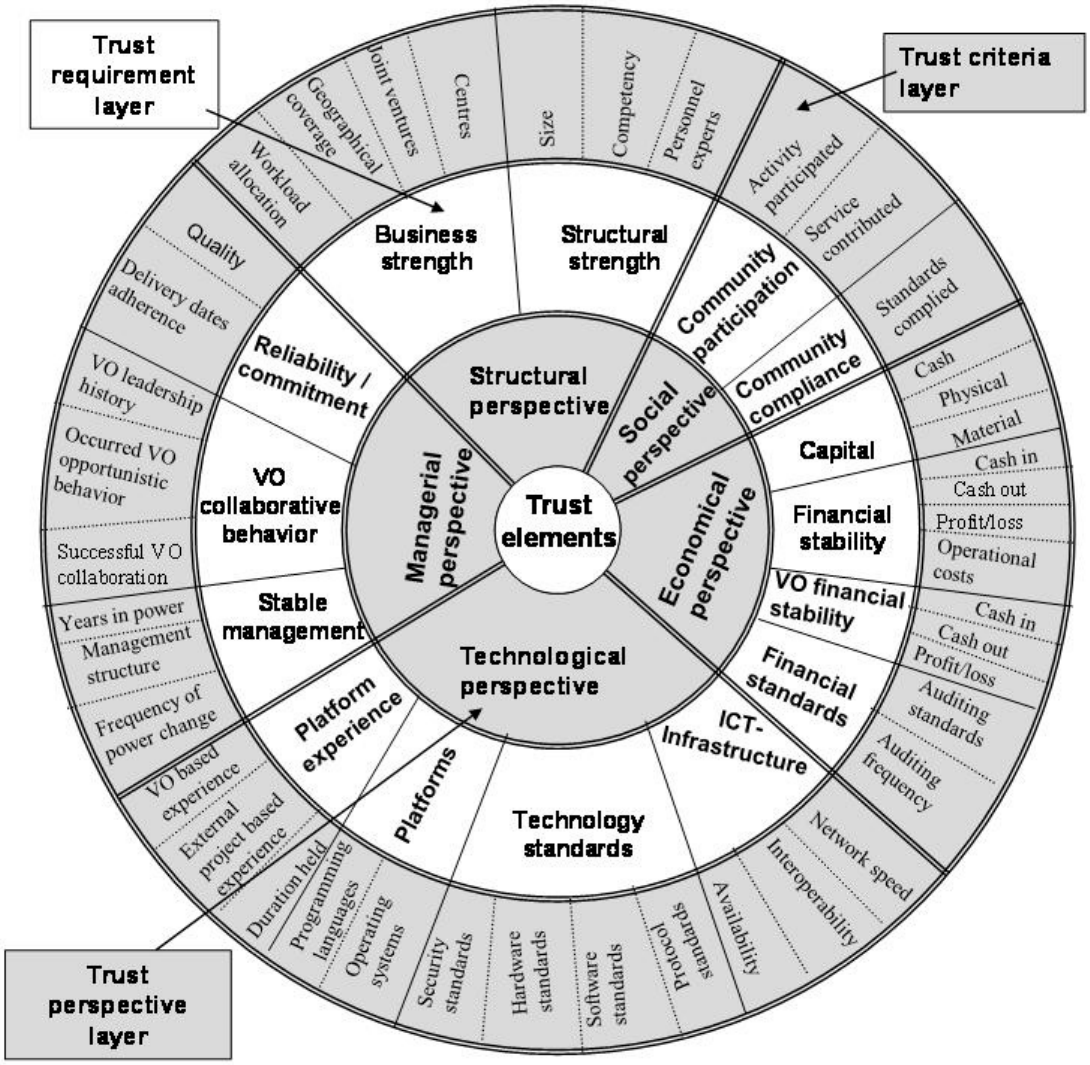

Figure 2: General trust criteria for organizations (Msanjila&Afsarmanesh, 2007a)

STEP 3: ASSESSING TRUSTWORTHINESS OF POTENTIAL MEMBERS

Designing and developing *rational (fact-based) mechanisms* for assessing the level of trust in organizations is of particular importance to large and very large CNs, in which all member organizations are not usually familiar with one another. This paper presents a conceptual model in terms of mathematical equations applied to rational analysis of trust level of organizations. The model is applied to develop rational (fact-based) mechanisms for supporting an objective trust analysis in CNs. That is to say, developed mechanisms are used to assess the level of trust in organizations. The model, and thus its related mechanisms for assessing the level of trust in an organization comprise measurable trust elements, namely trust criteria, known factors and intermediate factors.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

Known factors represent a set of domain/application dependent factors that indirectly influence the outcome of measurements of level of trust in the involved organizations. Each domain/application, such as business, manufacturing, medical, and so on, is affected by both the CN's internal factors (e.g. the minimum wage per hour for all organizations within the CN), as well as the CN's external factors relating to environment / market / society in consideration of the CNs scope both geographical and area wise.

Intermediate factors represent the factors that play an intermediary role in relating the CN's known factors to its organizations trust criteria. In principle, both trust criteria and known factors do influence each other.

Requirement analysis and empirical studies have identified that establishing trust between organizations is amenable for a smooth management of collaborative networks and an antecedent for CN's effective operational continuity. To ensure that every organization in the CN meets the minimum established trust threshold, indicators need to be developed and applied to establish a grading and ranking scheme for trustworthiness of an organization. The proposed indicators in this paper, comprise what we suggest as an organization's *"trust level or trustworthiness"*. Among others, following represent the main needs for assessing the trust level of organizations in the CNs:

- *As a strategy to enhance cohesion among member organizations within the CN:* The assessment of the base trust level of an organization in the CN and particularly, when applying for CN membership can be perceived as an examination which every organization must qualify in order to enter and remain within the CN. This may positively influence the cohesion among member organizations and their perceptions that they together belong to a group of trustworthy organizations. As a result, CN member organizations will perceive as operating in a controlled risk environment.
- *As a measure for management of the CN:* A key activity for a CN administrator is to ensure that member organizations meet all CN membership requirements necessary to assure successful CN continuity. Among others, such requirements include: possessing required competency, achieving good performance, maintaining proper ICT infrastructure for collaboration, and abiding to the CN working and sharing principles. Thus assessing trust level of each member organization in the CN will enable the CN administrator to have a general but complete picture about how the CN requirements are met by each organization. Assessing the base trust level of member organizations in the CN can thus be applied as one of the management measurement by the CN administrator. Thus assessing the base trust level of organizations within the CN indicates how the CN is prepared to compete in the market and in acquiring business opportunities, which are key aspects for its effective future continuity.
- *As an indicator for establishing objective-specific collaboration:* When a few organizations in the CN need to be selected for participation in a specific collaboration, such as in a consortium, their evaluated trustworthiness for the specific objective of the consortium needs to be measured. The selection of the most fit partner for each task considers the measurement of its trust level. These measurements indicate how trustworthy each member is when compared to other organizations.

As seen from the above examples about the need for assessing trust level of an organization in the CN, a wide range of trust criteria may be considered while evaluating organization's trustworthiness. Trust in CNs is characterized by considering a wide variety of aspects that together comprehensively support the rational measurement of trustworthiness of organizations. *As such, trust is not a single concept that can be applied to all cases for trust-based decision-making and its measurements depend on both the*

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

purpose of establishing a trust relationship and its specific involved actors. Trust level of an organization can be measured rationally in terms of quantitative values of related trust criteria e.g. based on an organization's past performance. The level of trust in an organization is complex and can neither be measured with single value of a single parameter, nor interpreted with a single metric. Nonetheless, an organization's level of trust can be specified on the basis of the values for a set of related trust criteria.

Understanding and interpreting the level of trust in an organization, described and formulated in terms of values of a set of trust criteria, will be complex and difficult to grasp for most decision-makers in organizations, such as managers and directors, if they are not trust experts and do not have sufficient knowledge in both mathematics and computer applications. Thus, the trust level of organizations must be presented in a format that is as understandable as possible to the expected users while not loosing its semantics.

This paper proposes that the level of trust in organizations should be represented and expressed in terms of a set of qualitative values, and these values can only represent comparative levels of trust in different organizations in a CN for a specific given trust purpose, and not as absolute levels. A set of "qualitative values" are designed for the level of trust in an organization to be presented to the decision makers that include: *Strongly more trustworthy, More trustworthy, Average trustworthy, Less trustworthy, and Strongly less trustworthy*. As an example, the comparative qualitative values of the trust level of four organizations (ORG-1 to ORG-4) in a CN are graphically represented in Figure 3. This representation is referred to as the "***Trust-Meter***". As shown in this figure, considering selected criteria, ORG-3 is "more trustworthy" that others.

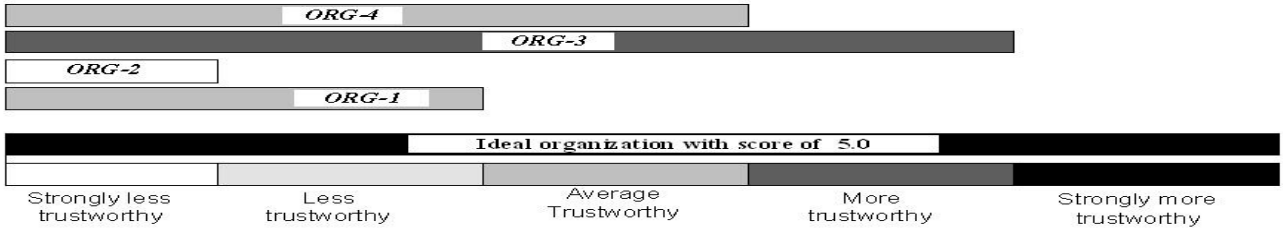

Figure 3: A trust-meter for presenting comparative level of trust in organizations

As such, in our approach the trust level of an organization is not an absolute value rather it is computed as a relative value depending on the following aspects:

- *Involved organizations:* While assessing the trust level of an organization, its relative score for each trust perspective is computed by comparing the organization's value for each applied trust criterion against the optimal value of that specific criterion, among the all involved organizations. The general equation below exemplifies how the relative score for the economical perspective (S_{ECO}) is computed from the values for its different criteria and the maximum value for those criteria.

$$S_{ECO} = f\left(\frac{capital}{\max\ capital}; \frac{financial\ \_\ stability}{\max\ financial\ \_\ stability}; \frac{VO\ \_\ stability\ \_\ stability}{\max\ VO\ \_\ based\ \_\ stability}; \frac{financial\ \_\ compliance}{\max\ financial\ \_\ compliance}\right)$$

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

Thus if some organizations join or leave the collaboration then there is a possibility that optimal values of some trust criteria may change. As a result the value for trust scores may change nevertheless, the relative scores of different organizations remain a good indicator for comparing the trust level of organizations. This illustrate that the trustworthiness of an organization is relative on the basis of involved organizations at the time of the computation.

- *Applied set of trust criteria:* In our approach the trust level of organizations is measured in terms of those trust criteria which are preferred and selected by respective trustors, depending on their: trust objectives, trust preferences and trust perceptions. Thus the relative nature of trust level of an organization also depends on these three aspects.
- *Grading and interpreting scores for the trust level:* In our approach, the score for the trust level of an organization is given in a range of zero "0" (representing the lowest score) and five "5" (representing the highest score). The intermediate ranges (namely, between 0 and 5) and their specific interpretation and meaning depend on the rating/grading of these scores as preferred by the trustor organization. Figure 3 shows an example of possible differences in setting the meaning to the range of scores assigned to different measurements of trust levels by different trustors. Thus the relative nature of trust is also dependent on the interpretation of computed scores by the specific trustor organization.

Please note that for the classification of different comparative levels of trust in organizations when specific ranges are not specified as exemplified in Figure 3, the *lowest resulted value* will be assigned to the category of "*Strongly less trustworthy*" and similarly the *highest resulted value* to the category of "*Strongly more trustworthy*" and the other categories represent a uniform distribution of these two values.

The score for the trust level of an organization is computed as a weighted generalization (e.g. averaging) of scores attained by the organization on the basis of specifically designated trust perspectives. With the base assumption, about the independence of the five trust perspectives, the generic formula is given below.

$$S_{TL} = Average\left(\left[w_{TEP} * s_{TEP}\right], \left[w_{STP} * s_{STP}\right], \left[w_{SOP} * s_{SOP}\right], \left[w_{ECP} * s_{ECP}\right], \left[w_{MGP} * s_{MGP}\right]\right)$$

Here, "S_{TL}" refers to the relative score for the trust level of an organization. The TEP represents technological perspective, STP represents structural perspective, SOP represents social perspective, ECP represents Economical perspective, and MGP represents managerial perspective of trust in organizations.

Furthermore, "*S*" (also defined further below) refers to the score that an organization acquires from the manipulation of its related values in each trust perspective and for the selected set of trust criteria for that perspective. Also, "W" refers to the weight specified for each trust perspective by each respective trustor organization. When weights are not specified, the Trust Management system, as introduced in Section 8, will assume uniform ones for all perspectives designated by the trustor organizations. The sum of these weights must always be equal to one and each weight must range between zero and one. Similarly, the score for each individual trust perspective, such as STP, will be calculated as a weighted

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

average of scores reached by an organization for each of the trust requirements in that trust perspective. For example, for the structural perspective will be calculated as follows,

$$S_{STP} = Average([w_{STS} * s_{STS}], [w_{BSS} * s_{BSS}])$$

Here, "*STS*" refers to structural strength and "*BSS*" refers to business strength, which together constitute the trust requirements of the structural perspective.

The *weighted average of the intermediate factorsrelated to each requirement* also applies to the calculation of the score for that requirement. While a number of generic intermediate factors that will be applied to all CNs are identified a-priori to a CN's establishment, and their respective formulas are predefined, in some case more specific intermediate factors might need to be identified and defined during the customization of the generic Trust.

STEP 4: PRESENTING RESULTS OF ASSESSMENT OF TRUSTWORTHINESS OF ORGANIZATIONS

One obstacle to the configuration of temporary consortiums as well as the management of collaborative network both involving new face organizations has been the difficulty in assessing and presenting the results of the trust level of involved organizations. The assessment and presentation of the results of trust level of organizations has been performed manually by trustor organizations and in ad hoc manners, which is both time consuming and hardly produces accurate results. Consequently, formation of collaborative initiatives in form of temporary consortiums has become more challenging and organizations are reluctant to work with each other. In this section we address the specification of services for automating processes related to the analysis and assessment of trust level of organizations.

Specification of system users and user requirements

Identification of users of the Trust Management system is based on the analysis of potential stakeholders for three general trust objectives regarding the creation of inter-organizational trust within CNs, namely:

- *Trust between CN member organizations:* This trust objective addresses the assessment of the level of trust in organizations and the establishment of their trust relationships for different purposes, such as smoothing cooperation in the CN, and enhancing collaboration in consortiums. The potential stakeholders for this trust objective are: CN administrator, consortium planner, CN member organizations, and CN membership applicants. Requirements for the organizations related to this trust objective are described in Table 1.
- *Trust between a CN member and the CN administration:* This trust objective addresses the creation of trust in a CN member organization towards the CN administration, as a means to: enhance the commitment of the member to the CN, ease managerial tasks, attract new member organizations to the CN, and so forth. The potential stakeholders for this trust objective are: CN administrator, CN member organizations, and CN membership applicants. The user requirements for the organizations related to this trust objective are described in Table 1.
- *Trust between external stakeholders and the CN:* This trust objective addresses the creation of trust in external stakeholders towards a CN, i.e. organizations that have been invited to become members or customers that wish to provide opportunities. The potential stakeholders for this trust

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

objective are: CN administrator, and external stakeholders (customers and invited organizations). User requirements for the organizations related to this trust objective are described in Table 1.

Five user groups are classified on the basis of these three general trust objectives. This classification is based on: each group's respective user requirements that need to be supported by the system, the rights for each user within the system, and the roles that these users will play in addressing a specific trust objective. These five User Groups (UG1 to UG5) and their respective user requirements are presented in Table 1.

Table 1: Identification and classification of users of the Trust Management system

User group	User roles & rights	User requirements (UR)
UG1: CN administrator	Highest administrative rights and can view, execute, modify all services	1. Assessing the trustworthiness of membership applicants and CN member organizations. 2. Defining, authorizing and assigning rights to other users. 3. Supporting other users, such as the consortium planer, in evaluating the specific trustworthiness of trustee organizations for certain purposes. 4. Managing the trust related data in the system. 5. Updating the list of trust criteria in the system.
UG2: consortium planner	Limited administrative rights and can view and execute some services	6. Viewing the trust criteria that are used in the system. 7. Selecting specific trust criteria from the CN pool of trust criteria. 8. Applying the selected trust criteria to evaluate specific trustworthiness of potential consortium partners.
UG3: CN member	Normal user rights and can manipulate its own records	9. Accessing its base trust level records 10. Updating its trust related data 11. Viewing the trust criteria that are used in the system.
UG4: Membership applicant	Basic user rights and can submit trust related data	12. Submitting trust related data as a requirement to the analysis of its membership application
UG5: External stakeholders	Guest rights and can access public information only	13. Supporting customers to analyze trust of CNs and thus trusting those CNs for purchasing their products and services. 14. Supporting invited organizations that want to become members in the CN to analyze the trust of that CN in relation to their businesses and possible benefits. 15. Guests to access on the basic information related to trust of the CN.

Another potential user is the *trust expert*. This is a specialized user which needs TrustMan functionality to support tuning the TrustMan system to match the requirements.

Specification of functionalities and services

In this section we address the specification of functionalities and services that shall be provided by Trust Management system. These specifications are based on the analysis and classification of user requirements.

A. Specification of required functionalities for the Trust Management system

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

The specification and design of the Trust Management system is based on the service oriented architecture (SOA) and in particular the web service technology. Accordingly, the specified functionalities are referred to here as services (referred to as "S" in table below). The system provides seven integrated services as described in Table 2 to support all user requirements as presented in Table 1.

Table 2: Specified services of the Trust Management system

S	Service name and description
S1	For assessing the base trust level of organizations: This service supports the assessment of trust level of an organization applying the set of base trust criteria, for two main purposes, namely: supporting the periodic assessment of base trust level of member organizations and supporting the one-time assessment of base trust level of a membership applicant. This is mainly a administrative service and it is accessed by the administrator of the collaborative network. The service also supports member organizations' assessment of their own base trust level.
S2	For evaluating the specific trustworthiness of organizations: This service supports the trustor NFO (administrator, or consortium planner) to evaluate the specific trustworthiness of an organization for a specific trust objective, such as inviting a CN member to participate in a temporary consortium, appointing a NFO member to become a consortium coordinator or the administrator of the collaborative network. The evaluation of specific trustworthiness can be done at any point in time, such as the current time. Furthermore, the evaluation can be used to forecast trustworthiness for future collaborations. This is an administrative service.
S3	For establishing trust relationships between organizations: This service supports an organization, based on its user rights, to access trust related data and decide regarding the suitable information to provide to other organizations in order to create trust. The challenge here concerns the provision of required information to create trust between organizations aimed at supporting the establishment of trust relationships. Therefore, it is related to five aspects, namely: "who", "when", "why", "what" and "how" (as further addressed in details in [Msanjila&Afsarmanesh, 2007a]). However, certain information that is stored in the system might be too strategic; as a result of which the owner organizations will be unlikely to allow it to be publicly accessed. In order to support this requirement, the access to trust related information is categorized as: (1) Public access – any organization may access the information, (2) Restricted access – any NFO member may access the information, and (3) Protected access – only the administrator of the collaborative network and the owner organization itself may access the information. This is a semi-administrative service.
S4	For managing trust related data: This service supports three kinds of users, namely: membership applicants, member organizations, and the administrator, for different purposes. The membership applicant will use this service to submit its own trust related data in order to facilitate the evaluation of its qualifications to join the collaborative network. The member organizations will use this service to update their own trust related data. The administrator will use this service to manage all trust related data in the system, i.e. to ensure that it is up-to-date, valid and extracted from a reliable source.
S5	For creating trust in the collaborative network: This service supports external stakeholders (customers and invited organizations) to create trust to the network establishment for different purposes. The external stakeholders need to access information that will persuade them of the trustworthiness of the collaborative network in relation to their businesses. The service also helps customers to build trust in the network in order facilitate business transactions, such as opportunity bids, payment procedures, and so forth.
S6	For managing the assessment mechanisms: The equations applied for the development of mechanisms for assessing level of trust in an organization incorporate some weights for the included trust criteria and the known factors. These weights may be changed from time to time when it is necessary. This service assists the consortium planner, administrators of the collaborative network and trust experts in adjusting these weights when necessary.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

S	Service name and description
S7	For analyzing an organization's trust-level history: This service supports administrator of the collaborative network to track the history or evolution of trust level of an organization. It has a mechanism that triggers the service for assessing base trust level for all organizations periodically (such as every six-months). The service then stores the results in the Trust Management database, the user can retrieve both the trust level history of specific organizations for a given period of time, and/or perform some analyzes such as identifying the weak or strong organizations.

6 Challenges and the future of the trustworthy organizations

Sufficient research has supported the current achieved conclusions, but it will never be enough to address future conclusions. Such future conclusions require further research in the future. Nevertheless, same future research topics can be defined in the conclusions of the current work. The subject of management of inter-organizational trust still has many open challenges that need to be addressed. We suggest the following four topics for future work in this area.

Analyzing statistical correlation for the use of trust criteria

Certain characteristics of the society and market might influence trustor organizations on their selection of trust criteria that are used to assess the level of trust in trustee organizations. For example, if an organization is doing business in a very socially-oriented community then adhering to social values of that society may seem more important than achieving healthy profits. However, in such a community there is an obvious risk of economic failure, such as failing to achieve the needed economic profit to survive. Thus, the trustor may need help to properly identify the needed criteria for trusting others. It is very difficult in general to predict or even analyze which trust criteria to use for each trust objective.

Nevertheless, when some trust criteria have been in use , in relation to certain objectives, for a relatively long period, this data can be recorded. Furthermore, collected empirical data related to trustee's performance can indicate if choosing certain trust criteria by the trustor instead of certain other trust criteria proves to be a good indicator of organizations' trustworthiness. Furthermore, certain trust criteria may not often be selected by trustor organizations. If this trend arises, it will discourage trustee organizations to pay attention to those less frequently selected trust criteria and thus they will not enhance their performance related to those trust criteria. However, this does not mean that those trust criteria may never be selected in the future. That means if they are selected, they might lower the trustworthiness of certain organizations, and may thus present an unexpected or uncommon organization's trust picture. It is in general unclear when and how these patterns relating to the selection of trust criteria by trustors will occur. Predictive studies or analysis of statistical correlations based on empirical data can support defining some indicators for the above example cases. Further research needs to be carried out addressing the above two aspects.

Complementing fact-based trust analysis with opinion-based trust analysis

This work addresses the research on rational trust for supporting the realization of trust between organizations on the basis of their fact-based data. There are however, a number of key practical challenges related to the application of rational trust analysis approaches in business. The following challenge has been identified to need further research:

Acquiring trust related-data on time: In our approach, the level of trust in an organization is rationally measured on the basis of a set of trust criteria. This means that updated trust related data for all preferred trust criteria must be available in order for the trust level of an organization to be computed.

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

In practice, however, when the amount of required trust related data increases, it may be hard to collect this data from organizations in time. Therefore, other complementary approaches, such as a subjective trust assessment approach can be considered in the event that trust-related data are missing for application of our rational approach.

Opinion-based approaches apply subjective data, such as reputation, to assess the trustworthiness of organizations. Although the base concepts of the two approaches, one rational and one opinion-based for analyzing trust differ the opinion-based approach may complement the rational-based approach when fact–based data are missing. In future research, when a new approach is introduced on how the results from rational trust analysis can be complemented with the results from subjective trust analysis, then the assessment results of the TrustMan system can be augmented with the results from other subjective systems. Furthermore, in future, other systems may be developed supporting rational analysis of inter-organizational trust that may be used by some organizations. For example, if some trust data of an organization related to one trust perspective of the TrustMan system is missing while another trust assessment system can compute the related scores for that trust perspective, then it may be possible to integrate those scores within the TrustMan system in order to provide a complete assessment of the trust level of the organization. In other cases, both TrustMan system and another trust assessment system might for example both generate some scores for certain trust perspectives, which may be also considered by TrustMan system. In either case, first the scores from another system shall be normalized according to the boundaries of scores generated by the TrustMan system, and second, the trustor organization shall set the weights for how it values the scores from each system.

7 Conclusion

Today's collaboration among organizations is continuously crossing political borders leading to complexity in formulating co-working networks of emerging new face organizations. Such co-working, which involves organizations that sometimes do not know each other, are difficult to manage and sustain due to the challenge of getting suitable partners. The effective smoothening factor in different forms of collaboration has proven to be getting trustworthy organizations.

NFOs need to build a trustworthy face towards other potential partners as well as towards the market. Thus these NFOs must pass the trustworthiness assessment test which is based on the measured criteria to enhance results rationality. Generally, the set of trust criteria applied to assess the level of trust in a NFO may differ among different trust objectives due to dissimilar perceptions and preferences on trust among trustor NFO. The preference of a trustor NFO influences its selection of trust criteria to apply in assessing the level of trust in trustee NFOs. Thus it is not possible to generalize for all trustors the selection of the set of trust criteria for all cases of trust establishment between organizations. Furthermore, the level of trust in an organization can neither be measured with a single trust criterion nor interpreted with a single metric. A multi-criteria approach is proposed in this work for assessing the NFO's level of trust. A large set of identified trust criteria for these new face organizations is also presented in this paper.

References

1. Afsarmanesh, H., Camarinha-Matos, L. &Msanjila, S.S. Virtual organizations breeding environments: key results from ECOLEAD. *In the proceedings of International conference on Cost Effective Automation in Networked Product Development and Manufacturing – IFAC-CEA'2007*. Monterey, Mexico, (2007).

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

2. Afsarmanesh, H. &Camarinha-Matos, L.M., A framework for management of virtual organization breeding environments, *In the proceedings of the Collaborative Networks and their Breeding Environments*, PRO–VE'05, Spain, pp. 35–49, (2005).
3. Blaze, M., Kannan, S., Lee, I., Sokolsky, O., & Smith, J. M. Dynamic trust management. *In IEEE Computer, Special. Issue on Trust Mangement, pg.44-52, 2009.*
4. Camarinha-Matos, L. M. &Afsarmanesh, H. Collaborative Networks: Value creation in a knowledge society. *In knowledge enterprise: Intelligent strategies in product design, manufacturing and management*, pg. 26-40, Springer, (2006).
5. Camarinha-Matos, L.M. &Afsarmanesh, H., Collaborative networks: a new scientific discipline. *In the International Journal Intelligent Manufacturing*, Vol. 16, pg. 439–452, (2005).
6. Clay, K. & Strauss, R. Trust, risk and electronic commerce. The 19th century lessons for the 21st century. *In the proceedings of the 93rd annual conference on Taxation,* National tax association and ecommerce, Mexico, (2000).
7. Cosimano, T. F., Financial institutions and trustworthy behavior in business transactions. *In the Journal of Business Ethics*, Vol. 52, pg. 179–188, (2004).
8. Currall, S. C. & Judge, T. A. Measuring trust between organizational boundary role persons. *In Organizational Behavior and Human Decision Processes,* Vol.64**,** No**.** 2, (1995).
9. Dasgupta, P., Trust as a commodity. *In Trust: Making and Breaking Cooperative Relations*. Basil Blackwell: New York. Pg. 49–72, (1988).
10. Grandison, T. &Sloman, M., A survey of trust in Internet applications. *In the IEEE Communication Survey Tutorial*, Vol. 3, pg. 2–16, (2000).
11. Good, D., Individuals, interpersonal relations, and trust. *In Trust: Making and Breaking Cooperative Relations*. Edited by D.G. Gambetta, Basil Blackwell: New York. Pg. 31–48, (1988).
12. Huynh, T.D., Jennings, N.R. &Shadbolt, N.R. 'FIRE: an integrated trust and reputation model for open multi-agent systems'. *In the* p*roceedings of the 16th European Conference on Artificial Intelligence (ECAI)*, Kluwer Academic Publishers, Valencia, Spain, pp.18–22. (2004).
13. Jones, S., Wilikens, M., Morris, P. &Masera, M. 'Trust requirements in e-business. A conceptual framework for understanding the needs and concerns of different stakeholders'. *In theJournal of Communication of the ACM*, Vol. 43, No. 12, December, pp.80–87, (2000).
14. Jøsang, A. & Lo Presti, S., Analysing the relationship between risk and trust. *In proceedings of Trust Management Second International Conference,*Oxford, UK, pp. 135–145, (2004).
15. Kini, A. &Choobineh, J. Trust in electronic commerce: definition and theoretical considerations. *In the proceedings of the 31st Annual Hawaii International Conference on System Sciences*, Kohala Coast, Hawaii, pp.51–61. (1998).
16. Mayer, R. C. Davis, J. H., Schoorman, F. D. An integrated model of organizational trust. *In Academic of Management review*. Vol 20 No. 3, pg 709-734, (1995).
17. Morgan, R.M. & Hunt, A. D. The commitment-trust theory of relationship marketing. *In theJournal of Marketing*, Vol. 58, pp.20–38. (1994).
18. Msanjila, S.S. Engineering the evolution of organizational trust in operating virtual organizations. In the international journal of the academic behavior management. ISSN – 1927-565X, Volume 1, pages 115-133, 2012.
19. Msanjila, S.S. *On Inter-Organizational Trust Engineering in Network Collaboration – Modeling and Management of Rational Trust*. ISBN 9789057761966, IPS drunkkers publishers, Amsterdam, 2009
20. Msanjila, S.S., Afsarmanesh, H. FETR: A Framework to Establish Trust Relationships Among Organizations in VBEs. *In the International Journal of Intelligent Manufacturing; Special issue:*

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014

Trust, Value Systems and Governance in Collaborative Networks. ISSN 0956-5515, Springer, (2008a).

21. Msanjila, S. S. &Afsarmanesh, H. Trust Analysis and Assessment in Virtual Organizations Breeding Environments. *In the International Journal of Production Research, ISSN (print) 0020-7543*, pg. 1253-1295, Taylor& Francis. (2007a).
22. Msanjila, S. S. &Afsarmanesh, H. HICI: An approach for identifying trust elements – The case of technological perspective in VBEs. *In proceeding of International conference on availability, reliability and security (ARES-2007),* pg. 757-764, Vienna, (April 2007c).
23. Msanjila, S.S. &Afsarmanesh, H. Towards establishing trust relationships among organizations in VBEs. In establishing foundation of collaborative networks – Proceedings of PRO-VE 2007, Springer, pg. 3-14, (2007d).
24. Msanjila, S. S. &Afsarmanesh, H. Understanding and modeling trust relationships in collaborative networked organizations. *In Business, Law and Technology: Present and Emerging Trends,* (Kierkegaard, S.M. –editor),Vol. 2, ISBN87-991385-1-4, pg 402-416, IAITL, (2006b).
25. Mukherjee, A. A model of trust in online relationship banking. *In the Journal of Bank Marketing*, Vol. 2, pp.5–15, (2003).
26. Povey, D. "Trust Management," http://security.dstc.edu.au/presentations/ trust/, (1999).
27. Rabelo, R.J., Gusmeroli, S., Arana, C., Nagellen, T.: The ECOLEAD ICT infrastructure for collaborative networked organizations. *In: Camarinha-Matos, L., Afsarmanesh, H., Ollus, M. (eds.) IFIP International Federation for Information Processing. Network-Centric Collaboration and Supporting Frameworks*, vol. 224, pg. 161–172, 2006.
28. Ratnasingam, P. Inter-organizational trust in business-to-business e-commerce: a case study in customs clearance. *In the journal of Global Information Management*, 2003.
29. Rousseau, D.M., Sitkin, S.B., Burt, R.S. &Camerer, C. Not so different after all: a cross-discipline view of trust. *In Academic Management Review*, Vol. 23, pg. 393–404. (1998).
30. Seigneur, J.M. & Jensen, C.D. Trading privacy for trust. *In Proceedings of Second Trust Management International Conference*, pp. 93–107, UK, (2004).
31. Smith, J. M. & Barclay, D. W. The effects of organizational differences and trust on the effectiveness of selling partner relationships. *In the Journal of Marketing, Vol*. 61, (1997).
32. Sztompka, P. Trust: A Sociological Theory. *CambridgeUniversity Press*: Cambridge, UK. (1999).
33. Weth, C. V. D. &Bohm, K. A unifying Framework for Behavior-Based Trust Models. *OTM 2006, LNCS 4275, pg. 444-461,* (2006).

ISSN 1923-0265 (Print) - ISSN 1923-0273 (Online) - ISSN 1923-0281 (CD-ROM), Copyright NAISIT Publishers 2014