Towards a Trust and Contract Management Framework for dynamic Virtual Organisations

Theo DIMITRAKOS[1*], David GOLBY[2], Paul KEARNEY[3]
[1]*Central Laboratory of the Research Councils, Rutherford Appleton Lab., OX110QX, UK*
[2]*BAE Systems Advanced Technology Centre, Sowerby Building, Bristol BS34 7QW, UK*
[3]*BT, Antares Building pp2/4, Adastral Park, Ipswich IP5 3RE, UK*

Abstract: TrustCom is a new European integrated project that aims to develop a framework for trust, security and contract management in dynamic Virtual Organisations. The framework will enable the secure enactment of collaborative business processes in self-managed, and dynamic value-chains of businesses and governments. The framework will leverage and extend the emerging convergence of open-standards, and in particular Web Services, and open Grid Services architectures. Validation will take place within industrial strength test-beds in the areas of collaborative design engineering (CE) and provision of ad-hoc, dynamic processes (ADP) for the on-demand provision of aggregate electronic services. This paper provides an overview of the TrustCom project vision, objectives and anticipated results.

1. Introduction

Recent years have seen an unprecedented acceleration in the evolution of the Internet as the technological vehicle underpinning the expansion of service provision and inter-/intra-enterprise integration in all market sectors. This brings about the prospect of *ad hoc* integration of systems across organisational boundaries to support collaborations that may last for a single transaction or evolve dynamically over many years. This sets new requirements for scalability, responsiveness and adaptability that necessitate the on-demand creation and self-management of dynamically evolving virtual organisations (VO) spanning national and enterprise borders, where the participating entities (enterprises or individuals) pool resources, information and knowledge in order to achieve common objectives. The objectives may be short term - e.g. to deliver a one-off service in response to a specific customer demand - or long-lasting. In the latter case, the VO's structure, business processes and operational infrastructure must adapt as the goals of the collaboration, the participating entities, the business context and the technologies employed, change.

Emerging ICT paradigms such as Autonomic computing, Utility computing and Grid computing are making the formation and operation of virtual organisations easier by providing dynamic management of the distribution of computational processes across available resources. However, the malleability of the digital medium that makes this possible is also a liability: a major limiting factor is a well-founded concern about exposure to fraud or misuse of the technology. Today, concerns about trust and security are acknowledged to be significant barriers to providing access to outsiders. Notwithstanding the major ICT breakthroughs of the last two decades, protecting one’s assets while integrating services, processes and resources, remains a major ICT challenge. Overcoming such challenges requires the development of disruptive technology realising innovative ideas over widely acceptable interoperable platforms. The required scalability, responsiveness and adaptability for on-demand created and dynamic virtual organisations, makes the provision of *cost effective* trust and contract management solutions for VO

---

[*] Contact Author: email: theo.dimitrakos@rl.ac.uk WWW: http://www.bitd.cclrc.ac.uk/Person/T.Dimitrakos

environments, *the* most demanding and timely research challenge in this field. Effective solutions require interdisciplinary approaches integrating tools from law, cognitive and social science in addition to telecommunications and computing. The successful deployment of *secure* and *trusted dynamic VOs* requires converging strategic research at a European level, coupled with mechanisms for integration of existing experimental results and the rapid dissemination, realisation and take-up of new research outputs.

The TrustCom project

In response to this challenge, the European Commission and a consortium of end-users, major software vendors and telecom operators, national research institutes and Universities, are implementing the new Integrated Project TrustCom. TrustCom will conduct multidisciplinary research in order to deliver:

1. *A novel trust and contract management reference architecture* that will enable collaborative work within on-demand created and self-managed dynamic VOs leveraging on the emerging convergence of Web Services and Grid technologies.
2. A set of *conceptual models* explaining the fundamental concepts, principles and methods underpinning the above architecture. Effectively these provide the meta-model of any new architectural constructs that may result from TrustCom research.
3. A set of *profiles*, that bring together and potentially extend selected Web/Grid Services specifications at specific version levels, along with conventions about how they work together to support potential implementations of the TrustCom framework.
4. *A reference implementation of the above* integrating and extending already established or emerging interoperability standards for autonomic security, trust and contract management based on Web and Grid services technology.
5. *System and software engineering tools and methods* analysis the VO life-cycle and offering a library of design patterns and generic software components implementing selected services that offer the core functionalities of the VO.
6. *Testbeds* exhibiting instantiations of the above architecture and reference implementation into two classes of realistic application scenarios, namely collaborative engineering (CE) and provision of ad-hoc aggregated services (ADP).
7. *Selected demonstrators* exhibiting the business value and benefits of the TrustCom framework in the abovementioned application domains.
8. *Studies analysing selected aspects of the legal and socio-economic context* that underpins such Virtual Organisations.

The TrustCom consortium

The TrustCom consortium provides a balanced blend of academic and applied researchers, end-user organisations, and enterprises looking to utilise results in products and services. As such it is well-placed to define, conduct and exploit leading edge research that is relevant to the needs of European business, government and society. The partners are: AtosOrigin (prime contractor), BAE SYSTEMS (leading the CE application area), BT (leading the ADP application area), CCLRC (responsible for technical management and scientific coordination), ETH, HLRS, IBM (leading analyses of the business and economic context), Imperial College (leading dissemination), King's College London, European Microsoft Innovation Center (leading standardisation), NRCCL (leading analyses of the legal context), SAP (leading exploitation), SICS, SINTEF, the University of Milano, and the University of Salford. For more information about TrustCom see www.eu-trustcom.com

2. Examples of Virtual Organisations in Collaborative Engineering

The development, production and support of modern products such as ships, aircraft etc are highly complex processes that often involve great risk. Principal risks include technical complexity (both in the complexity of products and processes) and changing customer and market requirements. The ability to manage these and other risks is a distinguishing feature of competitive organisations in the engineering sector. A strategy for managing this complexity is to form partnerships or Joint Ventures (JVs) in order to exploit new markets and opportunities through Collaborative Engineering (CE). In a JV partners focus on particular aspects of the product through its lifecycle, enabling more focus on core business capabilities. Emerging technologies such as web and grid computing may facilitate the evolution of JVs into Virtual Organisations (VOs), where organisations quickly come together to share resources without requiring the development of new facilities, and systems- a common feature of JVs at present. The CE scenarios described here attempt to cover most of the phases of the product lifecycle within a CE VO through development, production and in-service product upgrade.

The first of the scenarios focused on the collaborative design of a product in order to win a customer contract. The VO included principal partners who supply major sub-systems collaborating together to deliver a design that meets customer requirements and will lead to the award of a production contract. Customer requirements are negotiated and constantly refined and re-negotiated based on the results of the collaborative design activities. The VO also includes other collaborators who provide technical capabilities from High Performance Computing through to highly specialised engineering analysis services. Capabilities that currently reside within monolithic enterprises, and which are expensive to support, are outsourced and yet can still be integrated closely with the product development process within the VO. The benefits to the VO from this sharing of design data are improved understanding of customer requirements and reduced risk by more extensive design investigations using external specialist services. The interaction between partners' security policies that control access to the design data and collaborative agreements, defined at the business level, is an important issue in this scenario.

The second scenario focused on the management of complex engineering processes associated with the production phase. These processes span enterprises, potentially in different countries or economic zones and are possibly subject to export restrictions. Each partner providing a major sub-system (eg, engine, fuselage of a civil aircraft) also has a network of component suppliers and logistics support. These production processes are complex and may require re-scheduling in the case of delays in deliveries, etc. This may necessitate the sharing of process information (so-called 'process visibility') across the VO, entailing flexible security systems that control access to internal information. Other issues include the identification of trustworthy suppliers who can deliver components to time and specification in accordance with service level agreements.

The third scenario looked at the upgrade of an in-service airliner to include an in-flight entertainment system. The VO reconfigures to admit a new sub-system provider responsible for delivering this system. The new partner is also a member of other VOs, possibly competitors to the current VO. An important business decision concerns the trustworthiness of the product data- the new partner will need to establish the completeness and accuracy of the product data before it can plan its activities. A possible consequence here is the possible withdrawal of the partner from the VO if this data is of poor quality and poses unacceptable risks in delivering to contract. The new partner also wishes to monitor the in-service performance of the system using the customer's operations data. The security system of the new partner must be trusted by the VO to be sufficient to not allow sensitive product data to be accessible to its competitors; it must also be trusted by the customer to not disclose operations data to its own competitors.

In summary, the three scenarios have highlighted the importance of effective and flexible security system for building confidence in the extensive and more integrated collaborations that VOs offer over conventional JVs. The security policies should also be correlated both with the collaborative agreements established between partners at the business level and with agreements established within other collaborations as well. The benefits from an effective security and contract management framework are the ability for engineering collaborations to be quickly reconfigured in order to expose the assets that need to be shared to achieve the business goal. Service level agreement monitoring is important for ensuring that suppliers (of components, services etc) perform according to contracts. Benefits here possibly include the automation of processes between clients and suppliers that are usually repetitive. Finally, trust frameworks are required for supporting collaborations. The first of these concerns managing the reliability and trace ability of engineering data, ensuring that greater confidence can be given to it and that it can be relied on in major engineering tasks. The second of these Trust frameworks should facilitate the search for new partners/suppliers of components or services that were previously unknown to the VO. This should include some assessment of the trustworthiness of the security systems and its security policies.

3. Examples of Virtual Organisations for Next Generation Service Providers

We are interested here in VOs that are formed through ad hoc aggregation of component services offered by different 'real' service providers. Increasingly, enterprises are using web services and related technologies to provide their customers, suppliers and partners with direct access to their services and business processes. Motivations include reducing costs and speeding up processes through automation. However, the vision behind the web services / service oriented architecture revolution is that distributed applications can assembled as needed by connecting together pre-existing services. Selection of the services to use takes place through a 'discovery' process. As well as connecting the services together into a supply chain capable of fulfilling a customer order, the business process of the enterprises involved must also be interfaced. Furthermore, contracts need to be agreed establishing the the mutual rights obligations of the participating service providers. When connections at the these three levels can be established on demand, we can truly say we have an and hoc dynamic VO.

We are already seeing services being 'disaggregated', that is, in addition to offering 'complete' services, simpler constituent services are offered separately. Other organisations can then make use of these constituents in combination with their own service elements to offer composite services to their customers. Motivations for disaggregation include regulatory / anti-trust factors, advantages arising from focus on core competences, business agility (ability to launch new services / enter new markets rapidly), a desire on the part of the individual SPs to retain the advantages of small scale (or conversely to avoid the overheads and inertia of large organisations. New services may also be created specifically for use as constituents of larger services offered by other enterprises. This could offer opportunities for specialist start-up companies to enter a market. Benefits of dynamic aggregation include provision of services that are precisely tailored to a specific customer need. The need to offer a wide range of tailored services could arise from a wide range of preferences or requirements among the targeted customer base, or because the specifics of the service depend on the circumstance of the customer, e.g. current location, the task currently being undertaken, and other context specific variables. The ability to participate in dynamic VOs greatly increases the range of services a provider can offer to its customers, and also the number of end-customers it can reach indirectly via partners.

Five such 'Aggregated Services' (AS) scenarios have been defined and analysed as part of the TrustCoM problem definition: The first takes uses one of the ISTAG Ambient

Intelligence scenarios: 'Maria the Road Warrior'. This follows a near-future business traveller through her day, during the course of which she makes use of various services provided collectively by the many devices and systems making up the pervasive computing environment. We can see these services as being provided by virtual organisations forming in response to Maria's needs. The second scenario was similar, but less futuristic. A business traveller in a foreign city wants something to do in the evening. He calls into a WLAN-equipped café, and requests a personalised multi-media city tour guide to be shown using a combination of his personal computing equipment and the café's facilities. This service is provided by a VO consisting of the café, content providers / aggregators, the users 'home' service provider, and other network operators. The detail of the scenario focuses on the use of trust service providers representing the interests of the various parties. In the third scenario, a small software company wants to bid for a new contract, which under normal circumstances would be beyond the scope of its resources. The company has involved itself in a network of similarly placed small companies and is able rapidly to form a VO to compete with larger corporations in the development of new technologies. It is interesting to note that analogies can be drawn between this scenario and the TrustCoM project itself, raising the possibility that TrustCoM could be used as a test-bed for its own technology developments. The fourth scenario concerns experiential e-learning that may take advantage of a combination of semantic-based content selection, personalization of learning activities and integration with high-performance capabilities for virtual experimentation. Here, VOs providing highly personalised educational services are formed within a community of service, content and resource providers. A learner is assisted in defining a personalised training session, which is then enacted by the VO for the benefit of the Learner. The fifth scenario examines how a national or international incident (e.g. an environmental crisis) could be handled through collaboration among organisations that are selected according to context and must agree on a way of sharing and managing resources. As the resources and services are owned and managed separately by these organisations a decentralised command and control system will be advocated to synchronise their efforts and their use of the resources in the most efficient way.

In summary, the five scenarios have highlighted that dynamic VOs inevitably incur a management overhead compared to real organisations, and indeed to static VOs (formal consortia). There is a requirement for additional services to provide the glue that enables the VO to function as a viable entity e.g. to provide overall coordination of activities while retaining flexibility. We expect that these services can be defined in such a way that they are basically independent of the particular application domain. Furthermore, there is a requirement for services to replace the trust inherent in operation within an integrated real organisation (trust in colleagues   even when not known personally, trust in procedures and processes, etc.), and the trust between customer and an established service provider with a clear legal identity and brand / reputation. This last class of service is a main ingredient of the TrustCoM Framework. Without such a framework, it is likely that enterprises will judge that the risks in participating in dynamic VOs will out-weigh the benefits. Similarly, end-customers will be reluctant to buy from dynamic VOs. It should also be recognised that there are substantial commercial opportunities for enterprises offering the trust, security and contract management services instantiating the TrustCoM framework. The TrustCoM project will prototype implementations of potentially useful classes of service, drawing on the scenarios mentioned above for requirements.

4. An emerging common vision of Virtual Organisations

Based on the experience of the scenarios summarised in the previous sections, here we sketch the Virtual Organisations that TrustCoM innovations will help bringing about, emphasising some of the fundamental common characteristics that distinguish such emerging forms of VO from more traditional enterprise networks.

Virtual Organisations versus Enterprise Networks: A Virtual Organisation is understood as a temporary or permanent coalition of geographically dispersed individuals, groups, organisational units or entire organisations that pool resources, capabilities and information to achieve common objectives. Virtual Organisations can provide services and thus participate as a single entity in the formation of further Virtual Organisations. This enables the creation of recursive structures with multiple layers of "virtual" value-added service providers. The parties that form a virtual organization are typically part of a larger enterprise network of which a selection of partners is made. This phenomenon is known as "network activation" in VO modelling theory (See for example [18] and [13]). The entities in the Universe of such networks share some broad characteristics, e.g. belonging to the same economy or market sector, and their participation in the network indicates disposition to work together in a future market opportunity.

A common VO life-cycle model: The following life-cycle model[1] emerged as a reference, although it was noted that not all of these phases would necessarily fit the specifics of all VO variants considered in the project.

- *VO Identification*. This phase involves opportunity identification, opportunity evaluation and selection.
- *VO Formation*. This phase involves partner identification, partner evaluation and selection, and partnership formation, including the binding of the selected candidate partners into the actual VO.
- *VO Operation & Evolution*. This phase is characterised by the controlled integration of the services and resources, offered by the VO partners in VO-wide collaborative processes leading to the achievement of shared business objectives. Membership and structure of VOs may evolve over time in response to changes of objectives or to adapt to new opportunities in the business environment. Changes of VO context may necessitate contract amendment or adaptation of policy and business process enactment.
- *VO Dissolution*. This phase is initiated when the market opportunity is fulfilled or has ceased to exist. The major decision processes in the termination phase include operation termination and asset dispersal.

Targeted Virtual Organisations: This emerged as a characteristic of VOs that are formed and exist for a *purpose* [15] and in response to a *market opportunity* or in order to fulfil a *market demand* [10]. Consequently, the VO focuses on a particular market segment or target group. Targeted VOs are characterised by *goal-specificity* [14], i.e. activities and interactions of their constituents are coordinated in order to achieve explicitly defined goals that provide unambiguous criteria for selecting among alternatives, and by *deliberate cooperation* [14], i.e. the structure of relations between VO partners and the services and resources they contribute is made explicit and can be "deliberately reconstructed".

Dynamic Virtual Organisations: Membership and structure of such a VO may evolve over time to accommodate changes in requirements or to adapt to new opportunities in the business environment. While the VO as a collective collaborates towards a common objective, parts of the VO capacity and capabilities are owned by different independent partners, which have their own (partly overlapping, partly conflicting) interests. When the goal of a partner is met or the partner feels its own objectives no longer align with the goal of the VO, it can step out of the VO. Partners collaborating in order to perform a task in a phase of a VO may leave and join a different, potentially competing VO within the life-time of the former. The ability to self-organise is a key attribute of cost-effectiveness for dynamic VOs. A specific kind of dynamic VO are those that have the capability to unite

---

[1] Overall a similar life-cycle model has been used as a reference by the VOmap roadmap project "IST-2001-38379 Roadmap Design for Collaborative Virtual Organisations in Dynamic Business Ecosystems"..

quickly in order to exploit an apparent opportunity or common goal. We refer to this as *"on-demand formation of a VO"*. Dynamic VOs are particularly useful when faced with market incentives for responsiveness, dynamic service delivery, and charging based on usage. Beyond technological innovation, cultural adaptability in the organisation is essential for achieving an adequate degree of responsiveness.

Self-management of Virtual Organisations: Self-managed VOs are characterised by the ability to manage *at least* their operation and evolution without necessitating explicit intervention from the VO partners or other parties outside the VO. Self-management necessitates a form of integration that is enabled by the presence (or ability to form) an "autonomic" inter-organisational information system (IOIS) that supports the:

- *Negotiation and agreement of the conditions of involvement* of VO participants by means of electronic contracts whose operation is monitored and enforced by the IOIS;
- *Membership management and trust establishment* between the collaborating entities, be they the VO participants or the services and resources offered by the VO participants;
- *Specification, negotiation and distribution of policies* that control the sharing and aggregation of services and resources of VO partners in compliance with their agreement. Such policies need to be enforceable by the IOIS, and allow for adaptation (in real time) in response to changes of the context of interactions;
- *Specification, distribution and enactment of business processes*, which orchestrate the aggregation of information, services and resources in accordance to the consolidation of agreements between VO partners, VO-wide policies, and local (organisational) policies.
- *Resolution of conflicts or adaptation of VO operation* in response to alleviating the impact of violations of agreement or conflicts between policies, agreements, and business processes – both on the basis of their static description and their enactment.

The efficiency and effectiveness of self-management also depends on the extent that a VO achieves security and integration and in particular organisational transparency, shared leadership, and separability in VO operation and management.

Scalable Virtual Organisations: Scalability refers to the ability of the VO framework to be realised in different scales depending on its objective and the kind of the parties involved (e.g. large corporations, SMEs, solitary entrepreneurs). Scalability also allows the multiple interdependent layers of outsourcing as manifested by the constitution of recursive VO structures where similar VO formations may appear in micro- and macro- levels. This can be the case for example of a federation of providers offering high-performance end-to-end aggregate processes, where some activities are realised by aggregations of services provided by smaller-scale nested VOs and enacted over virtual execution environments which are also understood as VOs of execution hosts that federate resources in order to realise the enactment a service component.

Integrated Virtual Organisations: This characterises VO structures that comply with the typology of "dynamic networks" [16][17], as explained above, while they also support at least the following extreme aspects of an organisational network:

- *Organisational transparency* – meaning that although frequent and fine-grained interactions with customers are supported in order to facilitate mass-customisation, the co-operation of VO partners may not be visible to customers.
- *Cost-effective inter-organisational information system* (IOIS). A cost-effective IOIS requires the virtualisation of information and computation services and resources (at different levels of granularity) and their "just-in-time" integration across the boundaries of the VO partners. The formation of such a IOIS to accommodate the secure enactment of a collaborative business process within the VO should ideally take place at the time of demand. Its operation should respect the agreements between VO partners, the policies of the services and resource providers (who may maintain overall governance of the assets the provide to the VO) and the service and resource distribution should be transparent to the consumer both within and outside the VO;

- *Shared control* – meaning that while every partner contributes to the operational management of the VO, it does not automatically control the whole VO, although it effectively maintains high-level control within its own local administrative domain;
- *Shared leadership* – meaning that while every partner maintains control of their own assets and serves their own interests, these *must* relate to, and *may* be partly overlapping with, the interests of the collective.
- *Shared access to resources and services* – VO member may consume shared resources or services of other members for the purposes of enacting a collaborative task;
- *Shared loyalty* – entities within a VO constituency contribute to the common objective of the VO but also serve the specific objectives of their own organisation.
- *Mission overlap & co-destiny* – there may be partners that are also doing business outside of the context of the VO (and have a partial mission overlap) in addition to those (having a complete mission overlap) that all business is conducted within the VO context. In either case, the mutual dependencies due to the sharing or resources, services and knowledge and the shared risks make the VO partners also more dependent on each other, therefore necessitating collaborations based on a sufficient level of trust;
- *Separability* – meaning that VO management is characterised by clear distinctions between specification and deployment, and between a VO-wide "global" strategic management and a "local" operational management.

To achieve the desired economical performance, such "integrated" VOs require a functional efficient corporative network. VOs may be embedded in a larger network of corporations, from which certain members are recruited to deliver the required performances.

3 Anticipated Innovation

TrustCom innovation in supporting VOs will be centred around the following main themes:

- *Establishment of trust* relationships by means of digital identities, certification, reputation, and inspection to ensure the security, dependability and competency of the business partners,
- *Autonomic security*, including the specification, automated management and enforcement of policies controlling fine-grained access to the services and resources contributed by the VO constituents and assuring confidentiality / privacy, integrity, availability and accountability at VO level, while self-adapting to contextual changes within the VO.
- *Contracting*, focusing on the provision of trusted services to support the management of electronic contracts, the incorporation of guarantees to facilitate trustworthy collaboration, and performance assessment at the enactment of electronic contracts.
- *Business Process Enactment*, focusing on securing the enactment of collaborative business processes invoking services and consuming resources contributed by the VO partners in compliance with their security policies and agreements, and on self-adaptation to changes on the agreements contextual changes within the VO, including changes to the VO membership, security policy or agreements.

Research and technological innovation in the above themes will be informed by analyses investigating the legal and socioeconomic context of VOs:

- *Socio-economic Context*. Based on an empirical analysis of the market needs, TrustCom aims to develop new socio-economic models underpinning the establishment of digital economies within which VOs can evolve and generate profit. These will identify methods for creating incentives for engaging in trustworthy electronic collaborations and sharing services, resources information and knowledge within VOs in order to achieve common objectives in a way that multiplies their productivity and allows for the achievement of results that participants could not produce on their own.

- *Legal Context*. TrustCom will study selected legal and regulatory issues of collaborative work in VOs, focusing on privacy, data protection, and international issues. Analysis will also assess the expected impact of technological innovation in light of these issues and some legal and regulatory factors that could influence its exploitation.

4 Conclusion

In this paper we presented an overview of the motivation, objectives and approach of the TrustCom European project. More information about the project is available on the Web at www.eu-TrustCom.com and in this proceedings: paper [1] analyses indicative application scenarios, [11] refers to some relevant legal aspects, [3] focuses on the use and extension of Web Services Security technologies to assist the achievement of the TrustCom objectives. Papers [4][12][2][7] present partial solutions that may be reformulated and integrated in the context of TrustCoM. The project started in February 2004 and is expected to deliver the first version of its framework by the end of 2007.

References

[1]. Bernhard Katzy1, Gordon Sung, “State-of-the-Art of Virtual Organisation Modelling”. In Proc. Of eChallenges Conference. e2003

[2]. Chadwick David et al Extending/Adapting PERMIS to contribute to the TrustCoM objectives. eChallenges Conference: e2004.

[3]. Claesens Joris et al Investigating the Web Services Security framework as an enabling and extensible technology for trustworthy business processing in dynamic Virtual Organisations eChallenges Conference: e2004.

[4]. Theo Dimitrakos et al. Dynamic Security Perimeters for Virtual Collaboration Networks. eChallenges Conference: e2004.

[5]. Stefan Wesner , Theo Dimitrakos et al. Towards a platform enabling Grid based Application Service Provision. Challenges Conference: e2004.

[6]. Dimitrakos T., Valles J., Wesner S. The Grid for e-Collaboration and Virtual Organisations. In Proc. Of eChallenges Conference. e2003

[7]. Karabulut Yuecel Integrating a Unifying Trust Management Approach into Dynamic Virtual Organizations eChallenges Conference: e2004 (submitted).

[8]. Bernhard Katzy: Design and Implementation of Virtual Organizations. IEEE HICSS (4) 1998

[9]. Katzy, B.; Obozinski, V. Designing the virtual enterprise, Proceeding of ICE’99, 5thInt. Conf. On Concurrent Enterprising, The Hague, Netherlands, 15-17 Mar 99

[10].Kotler, Philip. 1994. Marketing Management. Englewood Cliffs, NJ: Prentice Hall

[11].Mahler Tobias et al. Reputation Systems and Data Protection Law. eChallenges 2004.

[12].Martino Lorenzo et al. eChallenges Conference: e2004 (submitted).

[13].Saabeel, W., Verduijn, T.M., Hagdorn, L., Kumar, K. (2002), A Model of Virtual Organisation: A Structure and Process Perspective, Electronic Journal of Organizational Virtualness, 4: 1. 2002

[14].Scott, W.R. (1998), Organizations: Rational, Natural and Open Systems, Prentice-Hall.

[15].Shao, Y.P., Liao, S.Y. and Wang, H.Q. (1998), A model of virtual organisations, Journal of Information Science, 24: 5, pp. 305-312.

[16].Snow, C.C., Miles, R.E. and Coleman. Managing 21st Century Network Organizations, Organizational Dynamics, Vol. 20, No.3, pp. 5--20. 1992

[17].Anne Powell, Gabriele Piccoli, Blake Ives. Virtual teams: a review of current literature and directions for future research. ACM SIGMIS 35(1). 2004

[18].Wassenberg, A.F.P. (1995), Netwerken: organisatie en strategie, Amsterdam: Boom Meppel.

[19].Wildeman L (1998), Alliances and networks: the next generation, International Journal of Technology Management, 15: 1/2, pp. 96-108.