7th WSEAS Int. Conf. on MATHEMATICAL METHODS and COMPUTATIONAL TECHNIQUES IN ELECTRICAL ENGINEERING, Sofia, 27-29/10/05 (pp13-18)

An Architecture for Monitoring and Coordination of Services in Networked Organisations

B. VASSILIADIS[1,2], J. TSAKNAKIS[1], L. DROSSOS[3], S. SIRMAKESSIS[1,3], K. IOANNOU[4]

[1]Research Unit 5, Internet & Multimedia Technologies,
Academic Research Computer Technology Institute
GREECE

[2]Computer Science, Hellenic Open University,
13-15 Tsamadou st. GR- 26222, Patras
GREECE

[3] Department of Applied Informatics in Management & Economy
Technical Education Institute of Messologi
GREECE

[4]Wireless Telecommunication Laboratory, Department of Electrical and Computer Engineering,
University of Patras, Rion 26500, Patras
GREECE

Abstract: - Success in the global market has made the adoption of modern management and administration structures of prime importance. The administration of heterogeneous sets of services and applications necessates the use of information technology, which facilitates cross-organizational process planning and tracking. In this paper we describe a Virtual Private Network architecture that uses special monitor and co-ordination processes in order to achieve efficient delivery of services and activities.

Key-Words: - Networked Organizations, Virtual Private Networks, Service Monitoring.

1 Introduction

The emergence of the "virtual organization" as an organisational form has evolved from a futuristic concept to an identifiable structure across a variety of organisations. Definitions of the virtual organisation share a common view of different organisations coming together as a newly defined unit. These virtual organisations are often incarnated as a virtual team made up of representatives from different organisations, often from differing physical locations, reflecting differing organisational cultures and providing different support services [1].

These descriptions of virtuality, in general, propose an entrepreneurial situation in which organisations or pieces of an organisational team exploit opportunities or take advantage of shared expertise, market access, or sharing of costs and risks. The co-ordination of services is critical to achieving the desired results of increased value added to both business processes and organisational mechanisms [2]. The “virtuality” of virtual organisations has been described as having two key features: creation of a common value chain between distinct entities and distributed, information technology supported business processes. For such practices however to become fully effective, support environments for the management and monitoring of communication fluxes between the various components is needed. Furthermore, these practises should be adaptable to the specific demands of different services in order to facilitate not only the evolution of the existing ones but the integration of new ones [3,4]. Grid Computing [5], Peer to Peer [6], Web Services [4] and outsourcing of IT [7] are the new business trends.

In this paper, extending our work in [8] to describe the architecture of an information standard system for the support of Virtual Enterprise Networks that use telematic services with similar characteristics that can be organised in categories.

The system supports a model that illustrates the interaction between suppliers, distributors, sub-contractors, customers and public authorities. According to the rules of this model, advanced services are adapted and integrated to a system, which can act in the network allowing the better synergy of composite groups of services in the information exchange and communication layer. This grouping of similar services in the communication layer, that is the common way of handling/scheduling their requests, significally increases request processing and makes better use of the available bandwidth.

The system's service oriented architecture provides a uniform way for transaction processing for entire categories of services. These services can be controlled in a transparent and co-ordinated way by several different actors –providers [9]. Furthermore, the system is able to autonomously activate and co-ordinate the sequence of operations and undertake automatic controls [10].

The main goals of the system are to:

- monitor and co-ordinate services and activities,
- disseminate new telematic services in order to enable and simplify dialogue between enterprises and public administration,
- promote integration among services creating an open platform in order to enable the electronic exchange of data and documents.
- reduce waiting time in communication

In this paper we discuss the general architecture of the system, emphasising on the solutions used to monitor and co-ordinate various activities. Sections 2 and 3 describes the value of doing electronic business transactions and briefly describes their mechanisms. In section 4 we describe the basic components of the system, the Virtual Private Network backbone, the Service Provision Component and the Public Component. Section 5 presents the conclusions and future directions of our on going research.

2 The Value of Electronic Business Transactions Systems

Many businesses are hesitant about taking steps towards developing electronic business transaction systems. Their main concern is the advanced technologies involved and their ability to master these technologies enough to implement them in a professional manner [2].

Experience has already shown that the use of these types of applications has much more benefits than the cost of the impact of changing the traditional way of doing transactions. This is a truth already known in the administrative staff of many companies who are already using such systems for a number of reasons [3].

Firstly, it appears to be a natural consequence of the evolution of IS applications and management in general, according to which electronic transactions may be regarded as the second phase of the systems integration trend, where applications for external business transactions are increasingly integrated to accomplish efficiency and effectiveness across the value chain.

Secondly, electronic integration can be thought of as shifting the boundary of an organisation out to include elements of other organisations, thus creating a "virtual organisation" of much greater complexity, the aspects of which should be investigated and analysed to gain a proper understanding of the complex environment within which modern enterprises operate.

Thirdly, another reason for the current attention on electronic business transaction systems relates to the ever-lasting aim of organisations to achieve "competitive advantage", particularly nowadays when the globalisation of trade has increased the number of competitors and firms complete in highly complex markets over wide geographical areas. Electronic business transaction systems, by enabling fast inter-border data flow, emerge as a "global technology" which can be used as a competitive weapon.

Finally, changing business practices and the emergence of strategies such as "just-in-time", Quick Response and Flexible Manufacturing, require even quicker responses and co-ordination of the logistical requirements, and these applications, by allowing this, have become a focal point for the achievement of "competitive advantage".

Of course the evaluation of use of such applications from a cost/benefit perspective is inherently difficult due to the intangible (strategic) nature of many of the benefits related to them. Similarly, while the essential elements of one-off and recurring electronic business systems expenditure can be directly identified (e. g. hardware, software, communications cost), other elements (e.g. the restructuring of internal processes) may be rather difficult to measure. International experience indicates that the application of electronic business transaction systems brings strategic advantages with reduced costs:

- improved communication speed which further leads to reduction of lead times and improved availability of data

- reduced paperwork which also entails simplification of both internal and trading procedures
- improved trading relationships
- improved customer service
- reduced operational costs
- gained competitive advantage through the support of a new business activity
- the way in which bank transactions take place as well as the procedures concerning exports will be shortened and enhanced
- operation expenses are considerably decreased due to the fact that a number of working persons are activated in other productive areas

Early electronic business transactions systems were developed using complicated applications which transferred standardised formatted data through telecommunication networks provided by private organisations or added value networks. However, in the last years, there is an intense trend for the utilisation of Internet as a mean for the development of such applications. The obvious advantages of this approach are the low cost of developing and installing Internet-based applications, and the simplicity of the WWW-based interface. Although the task of performing transactions through public access networks has a possible security hazard, encryption techniques can be applied in order to ensure information security.

3 The Business Transactions Mechanisms of a Virtual Enterprise

Our goal was to design a framework which deals, in an efficient and uniform way, with the various activities involved in the business transactions between a dominant enterprise and a large number of its subordinate suppliers which are located in dispersed regions (Business to Business model, figure 1).

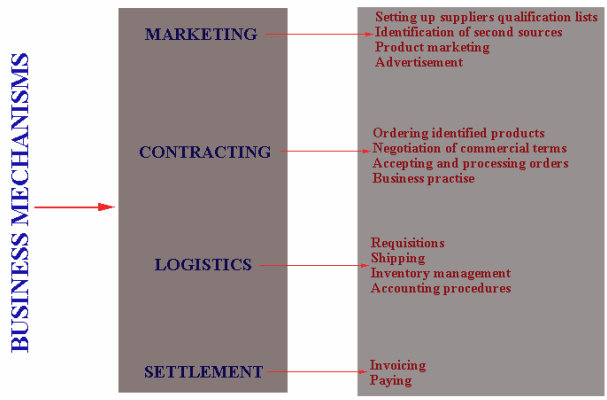

Figure 1. *The Business Transactions Mechanisms of a Virtual Enterprise [8]*

The main objectives of such an enterprise are:

- paperless exchange of information through he use of Information Technologies
- integration of Information Technology services for streamlining and optimising business functions.
- seamless transfer of data between business applications
- a new and more automated approach to trading partner relationships

The business mechanisms usually include the following transactions:

- Marketing. Marketing activities usually refer to selling, but for more and more purchases, marketing (i.e. identifying the best suppliers) is becoming a valuable activity in procurement. It includes activities such as setting up suppliers qualification lists, identification of second sources, product marketing and advertisement.
- Contracting. Contracting includes ordering identified products, negotiation of commercial terms, accepting and processing orders according to agreed terms and conditions and business practise.
- Logistics. Logistic include mechanisms that make products ordered available to the suppliers like requisitions, shipping, inventory management and accounting procedures.
- Settlement. Settlement activities include invoicing and paying for the products. They address the settlement of the trade and not just the settlement of payment instructions.

Business transactions take place within particular regulatory frameworks dictated by public authorities. All trading partners, the enterprise and the suppliers, need to interface with their respective public Administrations in order to obtain licences, certificates, pay taxes etc. Ideally, most of these activities should be undertaken by using electronic means but unfortunately most local authorities are still using traditional paper-based methods when interfacing with enterprises.

Business is traditionally contracted between partners who more or less trust each other. The level of trust may lead to different scenarios of the described model. High trust may entail payment being made a significant period after delivering goods. At the other extreme, low trust may require the use of letters of credit, where finance is being lodged through an intermediary. Authentication of both suppliers and the enterprise may become cost effective but valuable. In addition, since the provision of services will not leave traces or proof of service, mechanisms that keep track of service provision proofs in electronic form, paying

particular attention to integrity and confidentiality, need to exist.

4 The General Architecture of the Virtual Private Network

The system has three main components. A Virtual Private Network (VPN) which connects different actors (i.e. information system operators like enterprises and Public Administration Organisations) involved in the management and implementation of services. A Service Provision Component (SPC), which concentrates the interface on use, collecting the requests and distributing results. This component interfaces with the Virtual Private Network. A "Public" component for the dissemination of information. This component can be considered as "preliminary" to a category of services because it supplies information to external users.

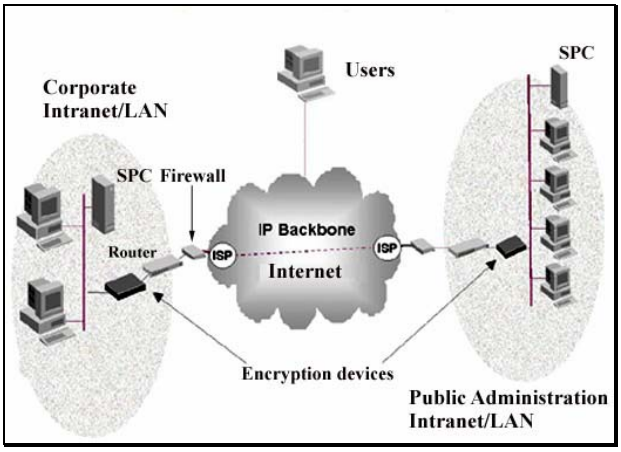

Figure 2. *General VPN architecture*

4.1 VPN Sub-system

This sub-system is used to receive service requests from users and distribute service activities among different bodies. The VPN sub-system supports the exchange of information among operators of different bodies and it also serves as an instrument of co-ordination among these operators. The various components are connected through Internet Service Providers (ISPs) to the IP Backbone (the Internet).

Current VPN architectures are based on two models: the directed VPN or the tunnelled VPN. Directed VPNs function at the session layer (layer 5) of the OSI network hierarchy. Directed VPNs offer unidirectional connections between corporate sites so the data exchange is highly controlled and monitored. A two-way trusted relationship is not assumed like it is with tunnelled VPNs. Tunnelling creates LAN-to-LAN or client-to-LAN connections at the packet level based solely on source and destination. Also, if security is breached in the directed model, only the destination network is affected. In the tunnelled model, the connections expose both the source and destination networks, so companies are more likely to inherit the security flaws of their VPN partners. In general, the higher a VPN is implemented in the OSI network model, the more secure it is because fewer changes are required to the network infrastructure. The trade-off is performance, which is better at the lower layers. In our case, the directed VPN architecture was selected since its more secure and permits controlling and monitoring of services and processes.

The transfer of confidential information through the VPN poses the need for security from outside intruders. The need for secure channels of communication and different levels of security was a major concern during the design of the VPNs architecture. In our case we used a three level security policy.

A good solution for the first level of security was the adoption of firewalls. While firewalls cannot prevent data-driven attacks, they provide control of the traffic that enters and exits the corporate Intranets/LANs. Traffic can be accepted or rejected based on application type and source address.

The second level of security is realised through the adoption of SOCKS v5, the IETF standard for authenticated firewall traversal, a standard proxy mechanism that resides at layer 5 between the network and application layers. It combines features from different levels of the network to offer a strong solution for securing data. It has the simplicity of the data-link solutions and the flexibility of
the application-layer solutions. Its inherent proxy capability allows extensive filtering of the data being passed over the VPN connection.
Finally, data encryption is used in order to encrypt user messages and credentials.

4.2 Service Provision Component

The SPC is the heart of the system and is responsible for co-ordinating and monitoring activities and services through the scheduling of request messages and/or information. The architecture of the SPC is presented in figure 3.

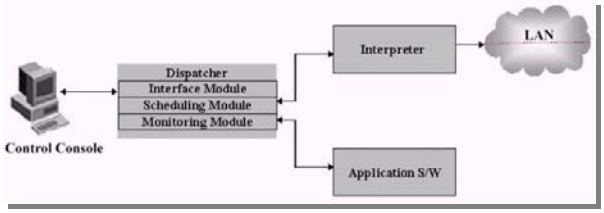

Figure 3. *The Service Provision Component (SPC) [8].*

Interpreter. This component transforms documents from internal format to the specific format of each workstation in the VPN. The use of standards for the exchange of data and documents enables high integration among services. Each message is constructed following a DIFACT standard using a randomly generated DES key along with MD5 data encryption. This technique ensures data security regardless of which network is used. A key is provided to all participating Intranets/LANs for them to be able to encrypt/decrypt their messages. This way, the sender of a message is always known by the key he is using. Keys are randomly generated and distributed to each participant in the VPN every month.

Application Software. The Application Software is dedicated to the automatic grouping of services that share common resources or exchange information with similar data types inside the VPN. Examples of such services include services which exchange multimedia information or services that use a specific database repository in order to retrieve or store information. The application software analyses each new service and groups it to an existing or new group according to the type of information that is exchanged (e.g. multimedia, text etc.) and the resources that must be used (e.g. an existing database with text information). The grouping process is semi-automatic. The service administrator uses the Control Console to set-up a new service. The user interface guides the administrator through the grouping process using a set-up wizard. A successful set-up requires the exact definition of every new service and its parameters.

The Dispatcher. The Dispatcher's main purpose is to perform scheduling and monitoring operations of the VPNs services. The Dispatcher consists of three modules: the Interface Module, the Scheduling Module and the Monitoring Module. The Interface Module provides a Web Front - End for the service and for the configuration application of the Control Console. The Scheduling Module is used for the routing of request messages of services between VPN Users, Databases, Control Consoles and Application Software. The routing procedures for each group of services depend on their configuration table.

Control Console The Control Console is based in a work station with which the body responsible for a service can monitor and configure it through the Interface Module of the Dispatcher. Each SPC has at least one Control Console. Control Consoles of multiple SPCs in the VPN can be used to configure only local LAN/Intranet services (e.g. Control Console of Intranet A cannot configure service x of Intranet B). Service configuration tables can be read - only by non - local Control Consoles or not accessible at all. Basic services or groups of services that are provided by all Intranet/LANs can be configured by one Control Console but copies of their configuration tables are stored in the Dispatcher of each SPC in the VPN. Each time the primary configuration table changes (for basic services it rarely does), the copies are updated. This policy of restriction over the configuration of services ensures the provision of unified sets of services with that remain constant for all the users inside the VPN. Of course, the efficient use of VPN services requires careful design and specification of every service.

4.3 The Public Component

This sub-system is responsible for the public distribution of information and services. These services are accessible via Internet connection by anonymous users. Only specific groups of services, the "public services", can be accessed by these users. Since there is no way of identifying external user identity and their intentions, an additional component is attached to the SPC, the Public Component. This component filters external user input and prohibits the use of information which is intended to be used by internal services only. Each public group of services has a separate configuration table which is stored in the Public Component. This table stores information concerning the resources that are publicly accessible for the Intranet/LAN they belongs to. This permits the distribution of different services/information per Intranet/LAN with different configuration on the public resources. If a data repository that is shared throughout the VPN is private for one Intranet/LAN then it is automatically inaccessible for external users.

Although we have included in the design of the VPN the possibility of provision of some basic services to external users (due to the possible participation of Public Administration Organisations to the VPN), our primary goal is the efficient provision of services to well defined corporate Intranet/LANs. The inclusion of external users to

such schemes, should be carefully examined due to serious security hazards.

5. Conclusions and Future Work

Virtual networks will challenge users with more than just boosting the performance on an individual network. Suppliers and customers will require a variety of automated services from VPN. Examples include direct customer sales and support via computer-telephone integration, electronic message transfers, and just-in-time product delivery with integrated inventory management systems. The technologies that underpin private and public virtual networking clouds are still evolving. The premise infrastructure decisions made today will affect the quality of performance and benefits well into the future. We believe that the architecture described in this paper is another step towards the customised/automated VPN. For many organisations this type of VPN will play an important role in advancing the cause of virtual organisations in the days to come.

The advent of networked business models has given rise to virtual enterprises, organisations comprised of geographically dispersed divisions and partners. In such situations, workflow management complexity has increased since processes use heterogeneous and dispersed resources. This situation entails the expansion of traditional workflow management practises, by taking into account the advantages of new computing paradigms such as the Grid and Service Oriented Computing.

References

[1] Rust, R.T., Kannan, P.K., E-service: a new paradigm for Business in the Electronic Environment. Comm. of the ACM, 46(6), 36-42, 2003.

[2] Handy, C., Understanding Organizations: Penguin, 2000.

[3] Jagannathan, S., Srinivasan, J. and J. Kalman, J., Internet Commerce Metrics and Models in the New Era of Accountability: Prentice Hall, 2002.

[4] Singh, P.M., Huhns, M.N., Service Oriented Computing, Semantics, Processes, Agents, Wiley Press, 2005.

[5] Foster, I., Kesselman, C., and Tuecke, S., The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of High Performance Computing Applications, 15(3), pp. 200-222, 2001.

[6] Androutsellis-Theotokis, S., Spinellis, D., A Survey of Peer-to-Peer Content Distribution Technologies, ACM Computing Surveys, Vol. 36, No. 4, pp. 335–371, 2004.

[7] Dibbern, J., Goles, T., Hirschheim R., Jayatilaka, B., Information Systems Outsourcing: A Survey and Analysis of the Literature. The Database for Advances in Information Systems, 35(4), 2004.

[8] Bogonikolos N., Tsakalidis A., Vassiliadis B., Giotopoulos K. and Likothanassis S., *"A Service Oriented Standardised System for Virtual Private Networks"*, Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications, pp. 360-366, Beirut, 2001.

[9] Currie, W., The organizing vision of application service provision: a process-oriented analysis. J. Information and Organization, 14, 237–267, 2004.

[10] Liu, J., Zhang, S., Hu, J., A case study of an inter-enterprise workflow-supported supply chain management system. Information and Management, 42(3), pp. 441 – 454, 2005.