The Impact of Security and Identity Management Issues in Grid: The Business Perspective

George THANOS[1], Eleni AGIATZIDOY[1], Karita LUOKKANEN-RABETINO[2], Igor ROSENBERG[2], Katarina STANOEVSKA-SLABEVA[3], Juan-Carlos CUESTA[4], Alan READHEAD[5], Ronald DOHMEN[6]

[1]Network Economics and Services Group, Athens University of Business and Economics, 76 Patission Str. Athens 11362, Greece, Tel: +302108203693, {gthanos, agiatzidou}@aueb.gr

[2]Atos Origin, Diagonal 200, 08018 Barcelona, Spain, Tel: +34934861818, {karita.luokkanen, igor.rosenberg}@atosorigin.com

[3]Mcm Institute of the University of St. Gallen, Blumenbergplatz 9, CH-9000 St. Gallen, Switzerland, Tel: +41712242793, Katarina.Stanoevska@unisg.ch

[4]Telefónica Investigación y Desarrollo, C/Emilio Vargas 6, 28043 Madrid, Tel: number: +34913374617, jcuesta@tid.es

[5]British Telecommunication plc, Floor 2 PP7, Antares Building, Adastral Park, Martlesham Heath, Ipswich Suffolk, IP5 3RE, UK, Tel: +441473646181, alan.readhead@bt.com

[6]T-Systems Solutions for Research GmbH, Postfach 50 01 44, 52085 Aachen, Germany, Tel: + 49 2408 943-5297, Roland.Dohmen@t-systems.com

Abstract: Security and identity management related issues indisputably constitute a major role in the adoption of new technologies in the Information Technology sector. Grid could not be an exception to that. This paper investigates another perspective apart from the technical one for dealing with such issues, the business one. It evaluates and discusses through real case examples, the risks associated with these issues in various heterogeneous industrial sectors, the impact of those in defining a successful business plan for a Grid product and the associated challenges. The aim is to provide a set of business guidelines and paradigms for early adopters not only for the Grid area but that can be also applied to associated, emerging and very promising technologies that Grid can be applied or integrated with such as Cloud Computing and Service Oriented Architectures.

1. Introduction and Objectives

Security and identity management are two of the key issues affecting the adoption of the modern Information Technology (IT) solutions in industrial settings [1]. Current trends like Service Oriented Architectures (SOA), Grid and cloud computing [2] for example presume that enterprises have to release information out of their administrative domains which raise (often doubtful) questions regarding to security of these solutions. Moreover, business models based on distributed computing, collaboration and virtual organizations assume high requirements for data privacy, where the credibility of data anonymity, authentication, and user authorization are among other things the critical factors defining the level of trust in the customers' minds, and their reluctance to adopt these solutions. Finally, the security requirements are not standard across industries, and might vary remarkably depending on the business focus.

This paper approaches the security-related issues from the business perspective in the context of Grid technology. The purpose is to find out what kind of role business specialists give to security and privacy issues, and in which extend they relate them as critical factors and risks for business success. The research presented here is a result from case studies of the Grid business experiments conducted as part of the BEinGRID (Business Experiments in Grid) project, one of the European Union's largest integrated project funded by the Information Society Technologies research. Nearly 100 consortium partners are running 25

Business Experiments (BE) which design, implement and deploy Grid solutions in different industrial settings.

The paper is organized as follows: the second section provides a description of the research methodology applied, whereas, the third section summarizes the findings from the literature research and presents a list of security-related issues in the adoption of Grid in business. The fourth section presents the results from the case studies regarding the impact of security-related issues in different industry sectors in a cross-case analysis and evaluation. Furthermore, it presents an example detailed analysis of one specific sector, the one that topped our evaluation in terms of high security risks and the way that these were dealt with. Finally, the last section concludes the document and proposes directions for future research.

2. Methodology

This paper assesses the security risks for Grid applications in business environments based on real-life cases. In order to achieve this goal first a literature review regarding potential Grid security risks and complemented with input from the market i.e. from the practical experiences of companies offering Grid products or related services, following our interactions with them as business consultants in the context of the project (over 80 industrial partners).

Next, these identified risks were assessed in specific business environments based on the case studies [3] of the BEinGRID. The experiments were clustered in industries such as the advanced manufacturing, media, financial, retail & logistics and eScience ones. First, the security risks were analyzed per experiment and then an aggregated summary per industry was provided. The main sources of information for the case studies were the various documented descriptions and presentations of the BEs, the analysis and review of the business and exploitation plans as business consultants of the project, and the bilateral communication with representatives from the BEs. The aggregated summary of identified security risks per industry was illustrated with a spider diagram. Besides the assessment of security risks also organizational and legal issues were considered as necessary measures that companies need to introduce to minimize security and identity management risks in a more holistic approach.

In a final step the findings were analysed based on the cross-case approach proposed by [4] and aggregated findings regarding security and identity management issues of Grid in business environments were summarized as well some advice given for potential adopters.

3. Security-related issues in the adoption of Grid in business

Grid technology provides powerful computing resources on demand, management of large amounts of data (storage, processing and distribution) and virtualized applications on top of a large scale federation of heterogeneous resources that may belong to different domains. This potential has been demonstrated in the scientific area and created an awareness and interest in Grid technology in commercial and industrial areas. High computing industries like finance, manufacturing, energy, health [5], life sciences and high distributed markets like retail, tourism etc, have already made first steps to adopt this technology. Despite the benefits, the market is clearly “hanging back” in regard to Grid technology because of business and technical issues related to the availability of applications ready for Grid, the migration costs of existing applications to a Grid environment, licensing, data privacy concerns, management of resources, reliability, maturity, dependability, security, availability of providers in the market, etc [6]. These concerns have prevented the widespread adoption of Grid solutions across the enterprises. A service provider for Grid-based services has to be aware of the real and perceived concerns potential customers have and address them in order to adopt a successful market entry strategy.

In the development of Grid computing within academic and science areas, focus has been primarily put on the implementation of a distributed high capacity computing platform. To enter the market, additional aspects like security need to be properly addressed. As Grid computing reaches a high level of deployment, the overload, systems and applications failures and the number of attacks that want to take advantage of the services or even prevent its operation will rise and can impact service levels. Regulatory bodies can establish additional requirements that can impose obstacles and/or barriers to the adoption of Grid solutions across national and/or international boundaries. Therefore, it is important for Grid computing to provide satisfactory solutions to the business need for high security including identity management and legal compliance. The economic benefits for organizations to share resources must be supported by the compliance with the security requirements in order for Grid computing to be accepted in the commercial sectors. Some of the security challenges that Grid computing has to overcome to cross from science environments to the main stream of IT services market we have identified are the following:

Usability: The adoption of Grid based services conveys a transition with technological and cultural changes. The step from in-house computing to shared and outsourced computing is also considerable taking into account the necessary mechanisms that have to be implemented to meet the required security policies and levels. The impact of these mechanisms must not affect the user experience. As an example, it's crucial to provide single-sign-on capabilities. This way, user authentication only needs to be done once.

Information privacy: Enterprises are very concerned about the risks they assume when their business data and resources are made available to external access, either because the company’s data is transmitted, stored or processed outside the company’s own firewall or their in-house resources (that they use for their business and in which they keep internal data) are shared with other organizations. Any issue about the confidentiality and integrity of the data has to be very clearly defined and solved [7]. Grid security must enforce the protection of the data confidentiality i.e. data should only be accessible to authenticated and authorised users and integrity as data won't be altered during communication processes by unauthorised access in the exchanges between the Grid and users and within the Grid.

Resource access and usage control: Grids are integrated by resources that are shared between organizations that can constitute a virtual organization. Organizations that contribute to the virtual organization by making available their resources are very concerned about the risks they assume when external applications are run in their resources. If their allocation is not controlled, resources can be unstable, unreliable or even unavailable; for instance, if an application consumes too many computing resources and starves other processes of resources. This behaviour can impact either the users or third-party organizations that also access the resources and are expecting to receive a contractual QoS. It needs to be clearly and carefully defined what is shared, the permissions to share, the usage patterns and priorities. The access authorization control to the resources must be based on credentials for the users, either global for all the resources shared within a virtual organization level with a centralized authorization system or on a resource level systems. The usage patterns and priorities can also be set individually for each resource or globally for the system and its application range from user specific to virtual organization wide resource usage patterns. These mechanisms must deliver QoS and prevent denial of service violations because of malicious users or application failures through the implementation of preventive measures.

Unified security: The unified implementation of the security schemes across the Grid is very complex because of the diversified environment. It's composed of computing resources with heterogeneous hardware and software platforms and security technologies that reside in different administrative domains with its own security infrastructure and different hosting environments. Interoperability is very challenging and requires the use of tools to hide this complexity without compromising performance.

Dynamic security configuration: The management of the Grid security must support the configuration of the security aspects previously described (information privacy, access and usage control) in an environment that is highly dynamic (creation of new services on-the-fly, deployment and withdrawal of resources, changes in the composition of virtual organizations etc), volatile and unpredictable. To adapt dynamically to the changes, security configuration management must be able to establish credentials and trust relations automatically, without human intervention, between virtual organizations, users, services and resources.

Management system: The management system is crucial to operating virtual organizations that may consist of multiple entities, components, users, domains, policies, and stake holders. Virtual organizations require a scalable, reliable and distributed management system capable of operating across organizational boundaries. This system must offer support for functions such as managing and safe storage of user credentials and trust relations and maintaining of group membership information. If this management is done at a user level instead of at the organizational level, security design can be very challenging.

Monitoring: Security policies implementation requires a system to survey resource usage and management system operations to create and negotiate trusts and authorize the users to access to resources. Apart from the security issues, monitoring is vital for several reasons. Most importantly, it provides the necessary information for charging the use of resources. Data gathered from monitoring is also needed for scheduling and QoS control. [8], [9], [10] describe the state-of-the-art of the different solutions to deal with these challenges.

4. Analysis of the impact of security-related issues per industry sector

As already presented, the BEinGRID BEs cover a set of representative industrial sectors that address concrete business cases and in which the main actors of the economic sector are represented. From a technical point of view, the BEs are using different Grid foundation middlewares, evaluating their suitability for solving specific real-world problems something that provided us with a more complete view on the real-life security issues. Furthermore, BEs stand as a reference point for other users. By highlighting the scenario, solution and result for each one of these cases, developing missing software and releasing best practice guides, our aim is to encourage other end users in a similar situation to investigate the role that Grid technology could have for them.

The 18 BEs (at the time writing this paper - currently 25) provide a wide variety of approaches of doing Grid-based business; this applies to the targeted markets as well as to the provided solutions and the business models. To analyse and evaluate the business potential and identify the areas that further improvement is needed across those heterogeneous approaches a specific analysis method was defined and utilised for all of them, which:

- focused on the essential business success criteria and their detailed analysis
- integrated the various business cases into a common analysis model in order to analyze and compare them in a reliable way
- included a ranking to evaluate the exploitation plans in a quantitative way

This method was based on well defined benchmark areas revealing how well each business case has managed to develop in each one of them. An analytical scoring tool was developed with detailed evaluation and scaling criteria. Finally, it was needed to find a visual way to present and compare results between different BEs. “Spider web” diagrams were considered as an appropriate way of doing this, as a commonly used tool in different contexts to analyse the important elements/factors of a topic under investigation, and to reveal the gap between the ideal level of development (or satisfaction) and current state.

Finally, in order to identify the problematic areas that need improvement in each business sector, a cross-analysis of the results was performed by comparing results of those BEs of the same sector. Such a per-sector analysis for the Grid area could not be found in the literature until now. Some of the areas analysed were the ones related to: product characteristics, target market, competition, financial aspects, strategy and implementation, risk and critical success factors and legal aspects.

The next sections present a discussion of the evaluation and comparison between the sectors as well as an example in-depth analysis for one of them as an illustration of the methodology used.

4.1. Discussion of results from the cross evaluation of all sectors

The processing of the initial results revealed some specific weak areas that were not tackled sufficiently enough especially when compared with the relevant technical documents. One area, as already mentioned was this related to the analysis of security and identity management issues. Despite the fact that one of the main concerns from the customer side was security, that seemed not to influence equally the products developed for the various sectors and the implantation strategy followed. A second round of analysis was performed in order to investigate further this. The analysis and evaluation produced the following result as seen in the next figure.

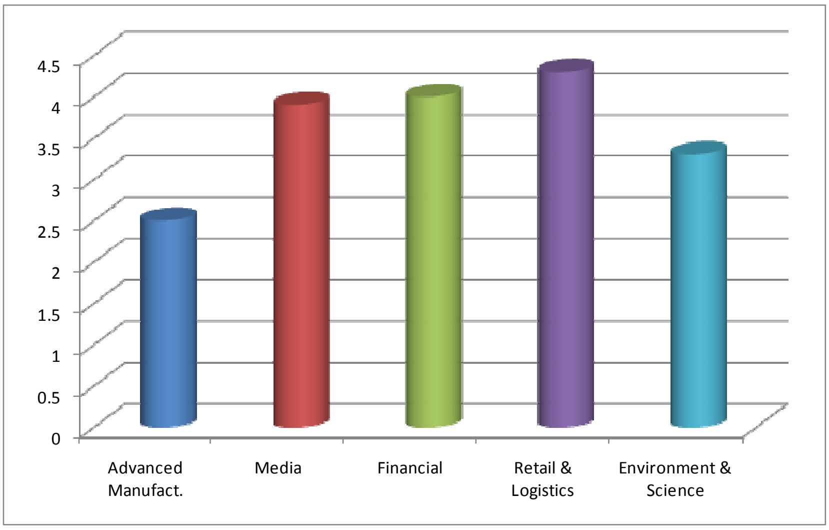


Figure 1: Evaluation of the (per-sector) significance of security and identity management issues in producing Grid business plans.

As it became apparent only 3 of these sectors took real consideration of the security and identity management issues around those cases: the retail and logistics, the financial and media ones. We found this to be attributed to the particularities of each sector (customer profiles, value-added of the products, target market etc), the IT-relevance and experience of the involved companies as well as to the different approaches followed in marketing the products. For example, the enhanced security promised through the usage of Grid middleware as a product feature in the financial sector products constituted a unique selling proposition highlighted in the marketing strategy of the product. In other cases such as the science sector, even though security was taken into account in the implementation/technical phase this did not affect their business plans, not even their risk analysis. It seemed that the business experts of the company either did not consult the application developers or that these issues were not spotted early enough to affect the business strategy development. Unfortunately, in some of these cases, as we now know, this early identification of security issues negatively influenced the success of the business plans due to the delays occurred in the implementation phase consequently effecting their financial figures.

The case studies of the BEs in the different industry sectors show that there are some differences in the experienced importance of different security aspects. The two main features of relevance for the retail and logistics sector are data exchange and collaboration among the companies involved in logistic supply chains. Thus, the main security risks experienced and scored by values higher than 4 are: information privacy, resource access & usage control and identity management. Ad-hoc logistic chains and changes in the flow of goods and information require in particular a sophisticated dynamic security configuration. Similar to the retail and logistics sector the main application area for Grid solutions is the collaborative work on media data. Consequently, the major security requirements identified in the involved BEs are: providing support for identity management, information privacy as well as resource access and usage control.

The focus of the Grid applications for the financial sector is on Grid solutions providing high performance computing for the various calculation models applied in the financial industry. At the same time data that might be prone to Grid computing is highly confidential. Thus, the main focus is on support for information privacy and identity management.

Grid technology needs to provide integrated solutions providing support for the combination of the above identified security risk in each sector. Our work has aimed to address security issues by emphasizing the fact that security is not important just technologically but the solidness of a technical solution has an important impact to business, and importantly, many market related issues give requirements and conditions to the technical solutions. Additionally, these requirements are not standard but might vary depending on a national, sector, and the business levels, and should be identified and analyzed from beginning. The following market and business related factors have been highlighted:

The regulatory rules and restrictions: The regulatory rules and restrictions (dependent on national laws and industries) can give the “go/stop –decision” for a new solution. For example in the health sector the patient privacy has to be guaranteed, and the solution has to be complete what comes to data anonymity regarding to patient information which goes out the hospital, authentication, and authorization.

The competition sensitive information: Firms are extremely cautious to give information about their customers and issues closely related to their core competences. This has a high importance especially in the cases where a service provider is having clients who are direct competitors, as well as in virtual organizations, where competitors are collaborating and competing at the same time. Thus, information privacy, resource access, unified security and dynamic security integration are the key for customers to adopt new solutions.

Consumer sensitive information: Even the most of the business cases develop solutions to a business-to-business context, the information about consumers might build their databases. In addition to strict regulations of data privacy, a solution provider has to convince the consumers that application is secure.

Customer orientation: Thinking, building, and communication the security issues from a customer point of view are the keys to reduce the customer reluctance to adopt new solutions. The goal should not be just on minimum requirements (e.g. technology and legal requirements) but to build the solutions which minimize the complexity, to be simple, and easy to understand.

The legal view: We strongly believe that the legal issues around security and identity management should not be underestimated. Contractual issues, Intellectual Property Rights, licensing, privacy and confidentially, software liability etc must be carefully investigated in the context of a new technology as existing practices may not be applicable. An overview of our legal analysis of these issues in the Grid context can be found here: http://www.gridipedia.eu/grid-legal-issues.html.

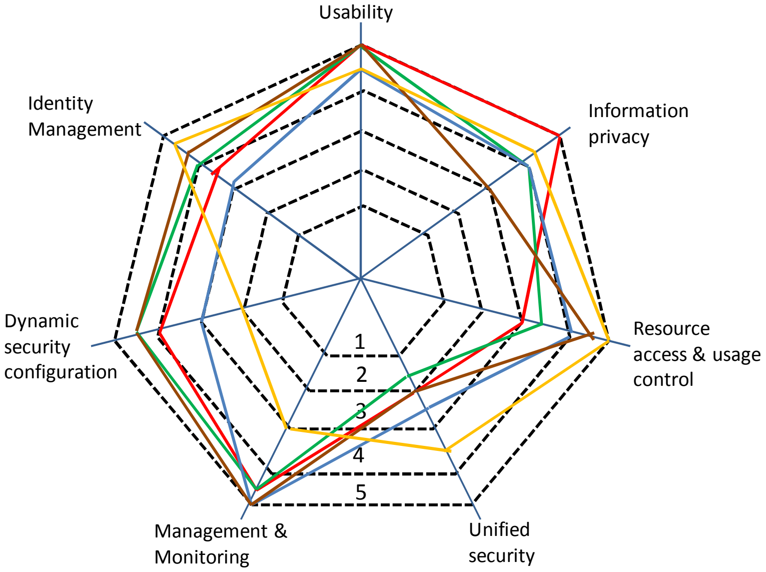
4.2. An example, more in-depth evaluation for the Retail and Logistics sector

This section presents as an example (due to the length restriction of the paper unfortunately we can not elaborate for more sectors) in more detail how the security and identity management issues were tackled by the Retail and Logistics sector that topped our evaluation. Furthermore, diagrams are used to present the impact of the different security risks discussed before.

The most significant key success factor for companies doing business in the Retail and Logistics market is the reduction of time-to-market, hence the optimization of the complete supply chain management, which includes procurement, partner management and asset management as well as production, delivery, retail and control processes across different locations. On top of that, a significant part of the companies and organizations doing business in the Retail and Logistics market are SMEs with limited resources to invest in those technologies which they crucially need in this highly competitive market.

There is a trend in the market, especially across SMEs towards the adoption of solutions to manage supplier collaboration, supply chain and demand planning to improve processes efficiency across the supply chain and the outsourcing of ICT services. Grid technology can help these providers to offer to their potential customers' innovative solutions that suit to their business needs and has significant potential to be the base for these solutions.

BEinGRID has classified 5 BEs as belonging to that sector: BE05, BE10, BE12, BE13 and BE17. Detailed descriptions on these BEs can be found in http://www.beinGrid.eu/be.html. Security and identity management issues seem to have impact in this sector. The business plans highlight the importance of these (see figure below) as indicated by the analytic evaluation from the project's business consultants and experts. Some of the specific security and identity management capabilities of the solutions as well as issues spotted and tackled are presented –per BE- in the next paragraphs.



Legend – BE05: red - BE10: orange – BE12: green – BE13: blue – BE17: brown

Figure 2. Evaluation of security issues & risks in the retail & logistics sector

BE10 - Collaborative Environment in the Supply Chain deals in particular with security and privacy issues. In particular, B10 in order to enhance its security and privacy features has made specific choices in their product implementation. First of all, it uses Gridsphere *(www.Gridsphere.org)*, an open-source portlet based Web portal. Gridsphere separates users and links them with one or more roles based on their responsibilities. For further securing the authentication process only 3 unsuccessful login attempts are allowed. In an effort to reduce the possibility of stolen cookies, portlet sessions are used, whereas in order to avoid sensitive data exchanges between machines an encrypted connection (https). In addition to the above, GRIA *(www.gria.org)* – the underlying middleware - uses off-the-shelf security components, including transport and message level security and dynamic authorisation linked to business processes and trust while they are firewall and network friendly. GRIA security is aligned with key web services specifications and supports transport level security using OpenSSL, message level security using WS-Security, access control rules use X.509 certificates and SAML, WS-Trust / WS-Federation pattern for client-side management, WS-Policy for describing message requirements, Dynamic policy enforcement point (PEP) and Dynamic policy decision point (PDP).

The BE10 prototype takes advantage of the public-key encryption technology and SSL allowing for collaborating sites to accept credentials while retaining local control. Furthermore, each user has a certificate and a Trade account which in turn contacts the SLA service. Through the SLA Management framework each organisation is able to control which services they consume, how much they are used, and by whom and thus enables trust establishment. The decentralized nature of GRIA allows for no single points of failure to exist, and thus if one GRIA site suffers a security breach, the problem can be dealt with locally. In fact, GRIA's low-dependency approach thus ensures a high degree of intrusion tolerance, which is essential for business Grid service providers [11].

The proposed solution of *BE12– Sales Management System Tecnocassa/Dominio* is based on the remote access to a database used by the applications and is designed to increase security. The technical improvements seem clear but there isn't a description of the business impact of this technical improvement or if this is enough for their customers to justify the adoption of the solution.

BE17 – Logistics and Distribution Optimisation addresses the creation of a scheduler/planner applied to logistic and transportation that integrates Enterprise Resource Planning (ERP) systems to reduce distribution costs. Particular attention has to be devoted to security and confidentiality. However, according to our view the business potential is relatively small and the value added is not clear.

5. Conclusions and further work

The main purpose of this work was the investigation of the role that security and identity management issues play from the business perspective in the context of Grid technology, and in what extend they constitute risks for business success. In order to accomplish our purpose we examined the relationship between security and identity management in Grid and analyzed the impact of security-related issues and associated risks in different industry sectors.

Security and identity management issues are strictly bounded with the distinctive characteristics of the various industry sectors. In many industries security has a secondary role, as the business experts focus only in the main advantages of Grid technology, such as the increase of the computational power. Nevertheless, there are industries, such as the financial or the retail and logistics, where the credibility of data anonymity, authentication and user authorization are critical factors for the survival of the enterprises. The main trigger for the adoption of security issues in those sectors are the market conditions as well as the regulatory rules or the sensitivity of the information either concerning the customers or the organization. Another important remark concerns the perspective by which security issues must be addressed. Those perspectives are technical, business, dissemination and legal, i.e. security must be tackled holistically and should be identified and analyzed from the beginning of the business plan.

We hope that our results motivate several directions for future research. The analysis was based on business cases that belong to different sectors. There are now eight more cases from proportional sectors (agriculture, health, telecommunications etc) recently incorporated in the project that will be integrated in our next analysis. Our aim has been for our results to be a guide for the incorporation of security issues into their implementation plans.

6. Acknowledgements

The research presented in this paper was part of the BEinGRID project (contract 034702), which is supported by the European Commission in the sixth Framework Program. Therefore, we would like to thank all the project's business consultants and experts for providing their valuable input and views in the analysis presented. Finally, we would like to thank Ms. Csilla Zsigri the ex-Activity 2 project co-ordinator for her efforts, as well as our lawyer, Mr Davide Parrilli for providing the legal insights in our analysis.

7. References

[1] Forge, S., Blackman, C., Commercial Exploitation of Grid Technology and Services - Drivers and Barriers, Business Models and Impacts of Using Free and Open Source Licensing Schemes, Final Report by SCF Associates for DG Information Society and Media, 25 November 2006

[2] Gartner, Gartner Voice, Understanding Cloud Computing, 25 June 2008c, http://www.gartner.com/it/products/podcasting/asset_202007_2575.jsp, access date: 8 July 2008

[3] Yin, R., Case Study Research - Design and Methods (2nd ed.). Thousand Oaks: Sage Publications

[4] Eisenhardt, K. M., Building theories from case study research. Academy of Management Review, 4(4), 532 – 550, 1989

[5] Chronaki, C.E., Chiarugi, F., Reynolds, M., Grid-enabled medical devices, Innovation in eHealth, and the OpenECG network paradigm, in Proceedings of ITAB 2006, October 2006, http://medlab.cs.uoi.gr/itab2006/proceedings/ECG%20Preprocessing,%20Analysis%20and%20Networking/144.pdf, access date: 24 July 2008

[6] The 451 Group, Grid computing preview, Section 7.2 (p. 83-89) in Review/Preview 2006-2007, The 451 Group, 2007

[7] Nagaratnam, N., Janson, Ph., Dayka, J., Nadalin, A., Siebenlist, F., Von Welch, Foster, I., Tuecke, S., The Security Architecture for Open Grid Services. http://www.cs.virginia.edu/~humphrey/ogsa-sec-wg/OGSA-SecArch-v1-07192002.pdf

[8] Xukai Zou, Yuan-Shun Dai and Yi Pan., Trust and Security in Collaborative Computing - Computer and Network Security Vol. 2, World Scientific Publishing Co. Pte. Ltd, 2008

[9] Yang Xiao, Security in distributed, Grid, mobile and pervasive computing, Auerbach Publications, 2007

[10] Grid Computing Security by Anirban Chakrabarti, Springer, 2007

[11] Andronikou, V., Kyriazis, D., Kardara, M., Halkos, D., & Varvarigou, T., Scenarios of Next Generation Grid Applications in collaborative environments: a business-technical analysis. In N. Bessis, Grid Technology for Maximizing Collaborative Decision Management and Support: Advancing Effective Virtual Organizations. IGI Publishing (Idea Group Publishing), May 2009 (to appear).