Identity and Access Management for Remote Maintenance Services in Business Networks

Kari Luostarinen, Anton Naumenko, Mirja Pulkkinen
Metso Paper, Inc., PO Box 587, FIN-40101 Jyvaskyla, Finland
Kari.Luostarinen@metso.com
Information Technology Research Institute, PO Box 35, FIN-40014,
University of Jyvaskyla, Finland
{Anton.Naumenko, Mirja.Pulkkinen}@titu.jyu.fi

Abstract. Access to information systems across corporate boundaries with high demands to privacy and trust result into ambitious research and development targets. This study provides motivation and a roadmap for approaching integrated security management solutions in a business network of partners with heterogeneous ICT and security infrastructures. We aim at describing specifics of identity and access management in inter-organizational collaboration, and a vision and arguments for identity and access management in a business network. A case study with Metso Paper, Inc., the leading manufacturer of paper machinery and related services, validates the results, thus providing a motivating example of the possibilities of e-services.

1 Introduction

Web technologies enable today ICT-supported business processes across enterprise boundaries [2, 11]. However, there are numerous questions to be solved before the information systems of collaborating partners can be set up and made accessible for the exchange of information independent of the geographic location of the provider and the clients. A core issue in building an e-services partnership is mutual trust [6]. To build trust, one of the first thresholds to overcome is the protection of the information systems and data from unauthorized access. In this case study, we examine an enterprise with both its own activities, and the sites of the clients distributed globally, and propose a roadmap for achieving an efficient and trustworthy user identity and access control management. The challenge is to provide secure ways and means to manage the user data and access control both within a geographically distributed enterprise, and for the collaboration with its clients at any location globally.

1.1 Background

We will refer to the business networks of multiple enterprises according to the definition of Rosenfeld [15]: The business network is "a group of firms with restricted membership and specific, and often contractual, business objectives likely to result in mutual financial gains… Networks develop more readily within clusters, particularly where multiple business transactions have created familiarity and built trust".

For an analytical view to the security infrastructure we use the four enterprise architecture (EA) dimensions Business Architecture (BA), Information Architecture (IA), Applications Architecture (AA) and Technology Architecture (TA) that find support in literature, especially practice related studies [4, 12-14]. To guide the EA management, planning and development, these dimensions are examined at different decision making levels with a narrowing scope of the decisions and respectively more specific level of abstraction. Three levels of abstraction have been found useful in practical EA work [17]: enterprise (strategic management), domain (management of operations; business units and processes) and systems level (information systems management). At the enterprise level, strategic decisions are made. At the domain level, the EA is developed in smaller units defined as domains (either development-time or permanent) with some decision making power delegated to them for more detailed decisions. At the domain level, the enterprise level strategic decisions are materialized into concrete designs of IT architectures and systems. At the systems level, detailed architecture descriptions are made, and fine grained guidelines, policies, patterns and standards for the systems are agreed on.

Today, business networking with web technologies requires management of architectures and business processes across organizational boundaries, both within large, global corporations, and between enterprises. The EA planning needs therefore to be extended to a multi-enterprise framework [8] with business processes supported by the architectures of the collaborating partners. Security issues come specifically into the focus at the corporate boundaries. However, the user data management (user identity and control of access to systems) within one enterprise is coherently controlled when embedded in a well managed EA providing a supporting framework for the enterprise security architecture.

The Identity and Access Management (IAM) area consists of two interrelated parts. The first part is the management of the users' identities that is basically creating, modifying and deleting of user accounts usually in a heterogeneous ICT environment. The second part is the access management which includes authentication and authorization services, management of access control policies, preferably a single sign-on (SSO) system, enterprise-wide access management, etc. [24].

The three areas make the basis of information security: authentication, authorization and audit. The authentication is the process of validating the credentials of a subject of access to guaranty subject's identity [3, 16]. The authorization is a right or a permission to use a system resource and it is the process of granting access [3, 16]. The audit is a review of logs in order to test the characteristics of security procedures, to ensure compliance with established policies and operational procedures, and to recommend any necessary changes [7, 16].

1.2 Metso Paper Inc.

The case company, Metso Paper Inc. specializes in pulp and paper industry processes, machinery, equipment and related know-how and after sales services. The company's offering extends over the entire life cycle of the process covering new lines, rebuilds and various services. Metso Paper's product range is the broadest in the field and covers the whole production chain from pulping to roll wrapping. The company vision is that Metso Paper unquestionably shall be recognized as the leading supplier of processes and services to the pulp and paper industry globally.

The information security issues relevant in providing services over the data networks accentuate the importance of managed enterprise architecture. Metso is an early adopter of cross-functional business processes and has implemented information systems to support them. The complete infrastructure has been built in sequential EA planning and development projects, which gives a readiness for constructing a consistent security architecture that can be extended also to cross-enterprise processes.

1.3 Related Work and Motivation

The paper provides motivation and a roadmap for approaching access control management challenges in a business network of partners with heterogeneous ICT and security infrastructures that together with high demands for privacy and trust result into ambitious research and development targets. This study describes the specifics of access control management, a vision, and arguments for federated access control management solutions in a business network. Research on the enterprise-wide security is richly available, for example Shaikh et al. provide a comparative analysis of existing IAM products and envision future needs of a next generation unified enterprise application security [20]. The works on the IAM in the area of virtual organizations especially using the service oriented architecture relate to the subject of our research and match the current setting of the industrial case [5, 9]. For example Weaver proposed a distributed data security via web services, trust and federation techniques for manufacturing and process industries [21].

This study extends the findings with new insights on challenges and impacts of IAM within the level of business networks and results to a concrete roadmap of research and development of access management solutions exemplified with the industrial case of Metso Paper, Inc. The instantiation of the roadmap using the real-world case of Metso Paper, Inc., improves the alignment of the research results with practical needs and constraints, serving as a motivating example for researchers as well as for ICT providers.

The paper follows in its structure the creation of a roadmap, starting with a vision, or the ideal situation with the access control management in a business network (section 2). Then, in section 3, the current situation and the steps to be taken with the security management for the company's business processes within the network are considered, according to the time axis. Section 4 presents the roadmap from the present situation to the ultimate vision analyzing and discussing the steps. Section 5 discusses the impact of the short-term solutions related to the identity federation. Section 6 summarizes the paper with conclusions.

2 Ultimate Vision

The ultimate vision, an ideal situation for the identity and access management, is here presented firstly, in general and secondly, with regard to the case of Metso Paper Inc. The vision of security infrastructure depends on and aligns with the vision for ICT, as presented at the enterprise level of the EA. However, some features of security are of major interest regardless of the ICT used.

In short, the ultimate vision of the business dimension (of the EA) is that trust between parties and privacy of partners are ensured by a proven high level of security embedded in the enabling ICT that automates business network processes. Security at the level of the business network can be ubiquitous and pervasive enough, mutating from an obstacle to a business opportunity and to an enabler of e-collaboration. Missions, business strategies and visions of partnering enterprises for trust and privacy have to comply with the cooperative mission, the alliance strategy, the vision and the security policy of the business network [6].

The business vision has to be supported with the information dimension by appropriate languages, structures and standards of data representation for formal, shared, flexible, expressive, distributed, and automated specification of business network access control policy. Formal specification refers to the need of having an access control model to mediate heterogeneity of policies and enforcement mechanisms. A shared policy has two features: the policy formats have to be interoperable in a business network and commonly accepted and understood by the partners. The security data structures and standards are flexible to accommodate the dynamics of the business network and technological changes. Heterogeneity of businesses, cultures, strategies, visions and approaches results in an important requirement to expressiveness of the access control policy language. The security infrastructure as presented in the information architecture of the EA has to support automated management of the access control policy in centralized, distributed and mixed architectures of the business network enabling diverse applications and technologies. The most challenging and promising among those architectures is the distributed management of the access control policies.

Information systems and applications at the level of the business network have to implement an access control model with features described above to support a distributed and cooperative management of access rights and user identities for the business network partners.

In the EA dimension of technologies, we need a new generation of authentication and authorization mechanisms that take into account the distributed and multi-owner nature of access control management. In addition to authentication and authorization there are a many other security solutions that need improvement.

Both technological and information systems security infrastructures have to be open enough to allow easy integration of all possible native implementations of security systems and technologies into a solid security infrastructure for a business network. Business network security solutions in all four dimensions of the enterprise architecture have to overcome heterogeneity of architectures of partnering enterprises. Strict alignment of the business network security architecture between all four dimensions and between enterprise architectures of partners is a key to a successful proceeding toward the ultimate vision.

3 Present Situation

For machinery maintenance purposes, the Metso Paper services unit has the need to access data residing in the systems of the clients of Metso Paper. These systems record data from the running paper machines at the paper mills.

Currently, Metso Paper has to send their own staff to install their own computer at the paper mill to be able to access the control systems that run in the client's network system. The clients' access policies are very strict and demand two persons to log in on Metso's computer.

Metso Paper uses Metso Secure Connection Solution (metsoSCS) for data transfer taking place between its network and its computer inside the client's network. The connections are built over public datacom networks with TCP/IP protocol as a VPN (Virtual Private Network) pipe through firewalls. In some cases the connection may be taken directly over modems. At the moment, most of the connections to paper machines are built using metsoSCS. Additionally, numerous tailored connections exist. However, only about 10% of the paper machines owned by clients of Metso Paper have a data communication connection with Metso. All connections go over the Metso Business Hub (eHUB) that directs the traffic between Metso network and the stakeholder networks, and is responsible for the authentication of the users and granting of access rights. Figure 1 illustrates Metso's Business Hub solution.

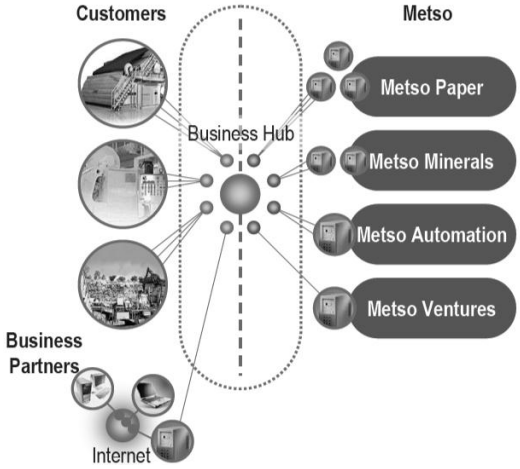

Fig. 1. Metso's ICT environment (adopted from [18]).

ICT environment of the business network has the architecture based on central and site business hubs for the remote maintenance of intelligent paper machines with embedded control and condition monitoring systems. Paper machines of Metso Paper contain control systems delivered by Metso Automation but in the general case could be operated using control systems of other vendors. The control system of Metso Automation follows enterprise application integration (EAI) technologies using service oriented architecture (SOA) [18]. Web services and a business process

management system are especially in use for condition monitoring purposes of Metso's experts. Together with maintenance functions, business hubs provide user management (at the central hub) and message security. With the current solutions Metso Paper assures that access to a customer's sites are limited to only Metso's users, the traffic to a customer's sites can be filtered at the Metso's end, the traffic is logged, user's traffic can be traced and reported to a customer. The authentication of Metso's users is done at Metso's site using the ACE/SecureID[1] and at customer's side based on a user's IP that has to be from Metso's pool of IPs; mechanisms of user authorization are not in use at customer's site at all; the logging brings into the correlation users and events of access to customer's network, leaving out of scope a purpose of access and actual activities during an access to control systems; the audit can trace only a time instance and a duration of user's access considering the whole IT infrastructure of a customer as a target of access.

The current setting is expensive because requires several servers, routers and firewalls both at Metso and at their clients. Almost every system and network solution the clients have are different and thus require tailored solutions. Existing isolated security solutions used by partners constrain and complicate the development of security infrastructure at the level of business network.

4 The Roadmap

Present situation without secure up-to-date IAM between Metso Paper and its customers is an obstacle for marketing remote maintenance services. This becomes the main business driver of enhancing the existing security infrastructure to the integrated IAM solution as a part of the maintenance service offering. The IAM has some unique features because of the situation on the IAM market and nature of the IAM offerings [23]. The IAM vendors provide suits of IAM components that result in a need to carefully make the first step and to define plans for long-term integration of enterprises and commercial applications [24].The integration is important strategic issue in the context of the Metso Paper case where clients have heterogeneous IT platforms and environments.

We consider interests of Metso Paper and its partners to motivate changes to their security infrastructures in short, medium and long term. Table 1 summarizes our findings and suggestions for the roadmap of a successful process of Metso Paper and partners to overcome trust and privacy concerns of all stakeholders with a solid, integrated and secure infrastructure in their business network. The proposed roadmap requires investments from all parties. This sets additional needs to motivate and keep in balance both the investments and the outcomes among the partnering enterprises. The roadmap suggests starting with the IAM components in the authentication field, followed by authorization related components and finally to conclude with the solid, integrated and secure business network centric IAM infrastructure. All components of IAM needed for the short and medium term goals are available on the market. They are sophisticated enough. Business network centric access control management as a long term goal is still a research problem for the academic world.

[1] RSA Security, http://www.rsasecurity.com/node.asp?id=1156

Table 1. The IAM roadmap for the business network of Metso Paper and its customers

Goal	Motivation
Short term	
Trusted authentication services of maintenance experts of Metso Paper on customer side: – Federation of identity from Metso Paper to customers. – SSO for maintenance experts.	Authentication of Metso Paper users at customer sites allows remote maintaining that can decrease total cost of ownership for customers and increase competitiveness of Metso Paper services. SSO is expected to allow maintenance using various devices from arbitrary locations.
Integrated authentication management and logging for audit.	Integration of authentication and logging mechanisms and systems automate and reduce cost of security management.
Medium term	
Trusted authentication services of customers for the product data management portal of Metso Paper: – Federation of identity from customers to Metso Paper.	The result is the trust in relationships between partners in the field of user authentication. Federated identity services in both directions allow creating of SSO by all partners. The solution enhances also customer loyalty and retention.
User provisioning – Partners facilitate provisioning of their IT resources to Metso Paper staff. – Metso Paper ensures secure provisioning of product data and services to customers. – Virtual directories integrate and synchronize user profiles and identity information from different authoritative sources.	Deployment of automated user provisioning solution impacts directly costs and improves quality of service level agreements by reducing time of request for access fulfillment. Automated disabling of accounts of terminated user enhances overall security and reduces risks of unauthorized access. Other benefits are the improvement of users' experience and saving in time.
Integrated logging for audit for newly deployed IAM components.	Integrated audit trail reduces risks and vulnerability of solid security infrastructure.
Long term	
Integrated IAM solution between Metso Paper and its partners based on federated extranet access management.	Business network centric IAM solution will fulfill business needs of cooperative partners.
Distributed and dynamic security architecture with improvements of tools for collaborative management of security and integration in all dimensions of business network architecture.	Involvement of all partners to the process of securing their business network raises shared trust and individual privacy that are drivers of long-term economically efficient cooperation.

5 Identity Federation

The identity federation is the first step and the basis for further elaboration of IAM in the business network according to the proposed roadmap. Figure 2 illustrates the place of identity federation in the overall architecture of remote maintenance services of Metso Paper.

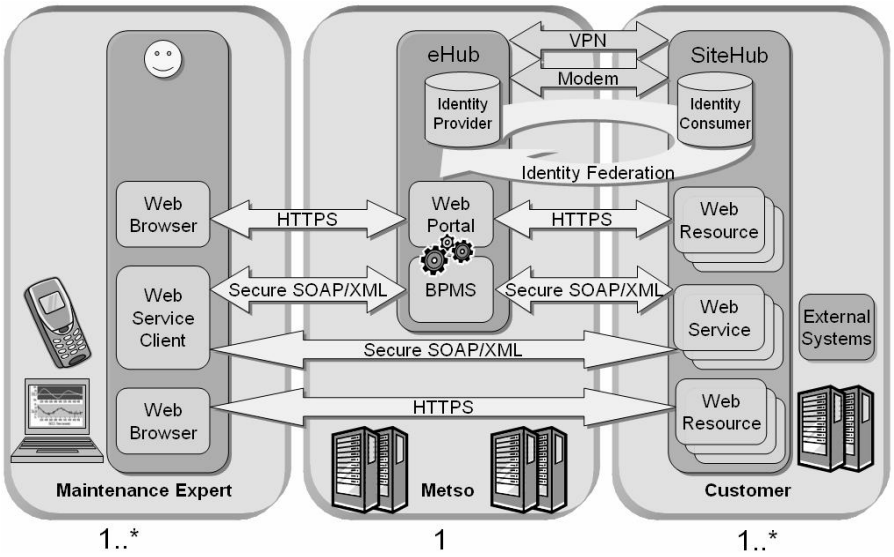

Fig. 2. The identity federation for remote maintenance services.

Metso's maintenance experts perform the condition monitoring remotely from desktop computers and mobile devices using web browsers and applications that access web services of business hubs. Currently connections are expensive and inflexible thus Metso Paper switches to protocols of secure communication using public networks like HTTPS for web browsing and secure SOAP/XML for applications based on service oriented architecture [22]. Metso Paper is going to employ the identity federation technology for providing SSO functionality for users and control over authentication, authorization and audit processes for customers.

There are three relevant open standards for the identity federation. The Liberty Alliance [10] is the project that delivers the framework for the identity federation with account linking, web service federating and linking of identity authorities. The security assertion markup language (SAML) [19] provides the identity federation functionality on the application level according to the well defined framework of sharing security information using XML syntax. The web service federation (WS-Federation) [1] is the specification of sharing authentication, authorization, attribute and identity information. WS-Federation is tightly relates to web service security, trust, policy and secure conversation standards.

Regardless of used standards, there are basically three possible options of the identity federation with respect to the distribution of accounts of users among federating partners. Figure 3 shows those cases.

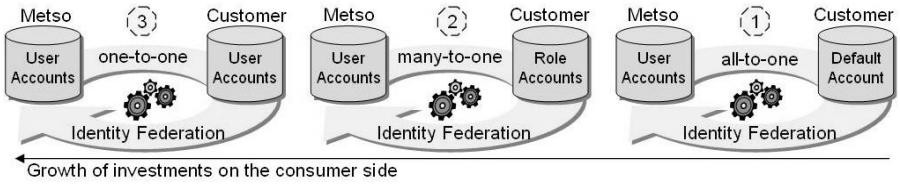

Fig. 3. Three options of identity federation.

The first option is a trusted authentication of Metso's users at customer's site based on public and secret keys without any account linking when Metso proves successful authentication and authorization of users by signing the security assertions or tokens with its secret key and customer provides access verifying the signature with Metso's public key. The second option is an authentication and authorization of Metso's users at customer's site based on role accounts which have links to maintenance experts' accounts at Metso's site. Third option is the user accounts linking when customers have copies of maintenance experts' accounts and authenticate and authorize like internal users.

We observed an experiment that was conducted by joint efforts of research group and representatives from companies to provide proof-of-concept evidences for the motivation of short-term goals. The experiment consisted of series of tests with the real-world identity federation products. The eTrust SiteMinder[2] was used to set up the identity provider server of Metso Paper and the identity consumer application of one customer. The PingFederate[3] was used as the identity consumer application of second customer. Despite of technical problems to run together products from different vendors that claim to comply strictly with the open standards, the results of tests proved in general that the short-term goals are feasible to achieve according to the proposed roadmap. The experiment validated and contributed to analytical conclusions about impacts of different options of identity federation architecture.

The analysis of impact of identity federation options for enabling SSO on the security level of customers factorized to authentication, authorization, audit and administration facets provided that

- one-to-one copying of accounts allow customers to perform authentication, authorization and audit of maintenance experts from Metso Paper like for their internal users, the only overheads appear for the administration part as the result of responsibility for accounts of Metso's experts;
- many-to-one option provides compromising solution of authenticating and authorizing experts based on separately created accounts on customer's site for experts' roles while names of real users could be provided for the logging and audit as part of assertion messages signed by Metso, the overhead again in the administration part is caused by role accounts and the key infrastructure;
- all-to-one option does not provide much improvement except again possibility to supply names of real users for the logging and audit process having overheads of keys infrastructure management.

[2] CA eTrust SiteMinder, http://www3.ca.com/Solutions/Product.aspx?ID=5262
[3] PingIdentity PingFederate, http://www.pingidentity.com/products/pingfederate

Impacts of identity federation options differ for Metso Paper and its customers. For example, copying user accounts to customer's site creates the threat of compromising Metso's security because of vulnerabilities of customers. Investments at Metso's and customers' sides grow along with the level of integration of user accounts from the first option to the third. Metso Paper will take investments even at customers' sites to its expenses because the security is considered as integral part of Metso's offering of maintenance services. Integrating and shifting of control over security related issues to customers rise the level of trust in Metso's business network while decreasing the level of security of Metso Paper itself. Thus Metso Paper does not consider any of identity federation options as the primary target for the development. Instead, portfolio of architectures which support all the options and typical control systems at customer's site, is the solution to achieve cost efficiency and satisfy requirements of customers to the security of remote maintenance services. The main factors for the decision about an option to apply in a particular case are the level of demands of a customer, its current IT infrastructure and mutual trust established already.

6 Conclusions and Further Research

The paper formulates the ideal situation of identity and access management in a business network by analyzing and decomposing it in an enterprise architecture framework of four dimensions: business, information, application and technology architecture. The proposed roadmap defines and motivates targets for further research and development of an integrated, solid IAM infrastructure exemplifying it on the case of a real industrial company and its business network where the provided services are enhanced with remote access to the clients' information systems.

The roadmap targets of short-term were evaluated during experiments with leading tools of IAM. The presented impacts analysis of different options of identity federation at the level of a multi-enterprise network is completed with the finding that none of the federation options is covering enough to substitute the others. Thus, the enterprise needs to provide a portfolio of security architectures that will be the target for more research and elaboration. This experience at Metso, a global large enterprise, could be of interest for other companies who consider federating of identities.

The case of Metso Paper serves as a trigger for further research. The description of the current situation, the envisioned ideal situation, long term goals and the business models of Metso Paper and its partners can be applied to similar settings. Further, they can be turned into numerous research questions, mainly in the area of security infrastructure integration and management of highly distributed, dynamic and heterogeneous ICTs at the level of multi-enterprise networks with high demands to privacy management solutions and trust. A major research area in the field of IAM is the data and application integration and its impacts in all EA dimensions within a multi-enterprise network as well as in adapting the network standards to the partnering enterprises. Further, there is a need for research on security infrastructure governance in a business network and on the alignment of an enterprise's and the business network's security policies and strategies. Information architecture security related models, languages and standards are expected to enable easy integration of business network centric IAM solutions. As for the application and technology

architecture dimensions of EA, there is a large area for more practical research on integration of different native security systems, mechanisms and tools.

Acknowledgement

The research has been conducted in the MODPA research project (http://www.titu.jyu.fi/modpa) at the Information Technology Research Institute (University of Jyvaskyla, Finland), funded by the National Technology Agency of Finland (Tekes) and industrial partners: Metso Paper, Nokia, SysOpen Digia, SESCA Technologies, Tieturi, and Trusteq.

References

1. S. Bajajet al. *Web Services Federation Language 1.0. Specification* (IBM, New York, 2003).

2. C. Britton, and P. Bye, IT, *Architectures and Middleware* (Addison-Wesley, Boston, 2004).

3. D. Ferraiolo, D. Kuhn, and R. Chandramouli, *Role-Based Access Control* (Artech House, Boston, 2003).

4. W. Hasselbring, Information system integration. *Communications of the ACM* **43**(6), 32-38 (2000).

5. M. Hatala, T. Eap, and A. Shah, Federated Security: Lightweight Security Infrastructure for Object Repositories and Web Services, in: *Proceedings of The International Conference on Next Generation Web Services Practices (NweSP'05)*. (IEEE, Piscataway, NJ, 2005).

6. J. Heikkilä, M. Heikkilä and J. Lehmonen, Sharing for Understanding and Doing for Learning: An Emerging Learning Business Network, *The ICFAI Journal of Knowledge Management* **3**(1), 28-45 (2005).

7. D. Kienzle and C. Elder, *Final Technical Report: Security Patterns for Web Application Development*. (DARPA, Washington DC, 2002).

8. A. Lapkin, *The Gartner Enterprise Architecture Framework. ITXPO Symposium*. (Gartner Inc, Stamford, CT, 2003).

9. Y. Lee, A Dynamic Virtual Organization Solution for Web-Services Based Grid Middleware, in: *Proceedings of Sixteenth International Workshop on Database and Expert Systems Applications* (IEEE, Piscataway, NJ,2005).

10. Liberty Alliance Project web site, http://www.projectliberty.org/.

11. D. Linthicum, *Next Generation Application Integration: From Simple Information to Web Services* (Addison-Wesley, Boston, 2004).

12. META Group Inc, *Enterprise Architecture. Desk Reference*. (Metagroup, Stamford, CT, 2002).

13. The Open Group, The Open Group Architecture Framework (TOGAF) Version 7 "Technical Edition", Version 8 "Enterprise Edition".Document Nr 1911 (The Open Group, 2002). Accessed 13.01.2004 at http://www.opengroup.org/togaf/ .

14. C. Perks and T. Beveridge, *Guide to Enterprise IT Architecture* (Springer, New York, 2003).

15. S. Rosenfeld, *Industrial Strength Strategies: Regional Business Clusters and Public Policy* (Aspen Institute, Washington, DC, 1995).

16. D. Russell and G. T. Gangemi, *Computer Security Basics* (O'Reilly & Associates, Sebastopol, CA, 1991).

17. M. Pulkkinen and A. Hirvonen, EA Planning, Development and Management Process for Agile Enterprise Development, in: *Proceedings of the Thirty-Eighth Annual Hawaii International Conference on System Sciences. Big Island, Hawaii, 2005*, edited by Sprague, R. H. Jr. (IEEE, Piscataway, NJ, 2005).

18. J. Pyötsiä, ICT opportunities and challenges for remote services, in: *Proceedings of the 1st International IFIP/WG12.5 Working Conference on Industrial Applications of Semantic Web, August 25-28, 2005, Jyvaskyla, Finland* (Springer, IFIP, Dordrecht, 2005), pp. 213 – 225.

19. OASIS Security Services TC, *Security Assertion Markup Language (SAML) v2.0*, , http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, (Oasis, Billerica, CA, 2006).

20. R. Shaikh, , S. Rajput, S. Zaidi and K. Sharif, Comparative Analysis and Design Philosophy of Next Generation Unified Enterprise Application Security, in: *Proceedings of The International Conference on Emerging Technologies* (C@SE, Islamabad, 2005).

21. A. Weaver, Enforcing distributed data security via Web services, in: *Proceedings. WFCS 2004 IEEE International Workshop on Factory Communication Systems*, (IEEE, Piscataway, 2004).

22. OASIS-Open Org. *Web Services Security, SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification* (Oasis, Billerica, CA, 2006).

23. Witty, R., Allan, A., Enck, J., Wagner, R., *Identity and Access Management Defined. Gartner Research Note SPA-21-3430* (Gartner Inc, Stamford, CT, 2003).

24. Witty, R., The Identity and Access Management Market Landscape, Gartner Research Note COM-21-4534, (Gartner Inc, Stamford, CT, 2003).