

SECURING VIRTUAL ENTERPRISES: REQUIREMENTS AND ARCHITECTURAL CHOICES

Paolo Spagnoletti
LUISS Guido Carli University
Via T. Salvini,2 – 00197 Rome, Italy
pspagnoletti@luiss.it

Stefano Za
LUISS Guido Carli University
Via T. Salvini,2 – 00197 Rome, Italy
sza@luiss.it

ABSTRACT

Cooperative environments where multiple organizations interact for providing e-services to their customers are widely diffused and often referred as virtual enterprises. IT systems supporting these inter-organizational models must be designed by taking into account both functional and non-functional issues. Among the non-functional issues, information security solutions play an important role as mechanisms for reinforcing trust among members of a virtual enterprise and their supplier/customers. In this paper, we outline a set of non-functional requirements for IT systems supporting virtual enterprises, and describe the federated identity management system which has been implemented in the context of an EU project (LD-CAST) as an example of a trust-reinforcing mechanism.

Keywords: Digital Platform, Identity Management Systems, Virtual Enterprise, Circle of Trust

1. INTRODUCTION

The increasing needs for complex products and services in competitive markets require new cooperative models based on networked forms individuals, communities and organizations. In this context, the interoperability of systems and organizations, enabled by standards and technologies, represents a central requirement towards flexibility, a strategic

attribute for competitive organizations¹. Several contributions in the organizational literature identify virtual enterprises as innovative configurations able to increase the benefits of inter-organizational cooperation².

A Virtual Enterprise (VE) can be defined as a “temporary organization of companies that come together to share costs and skills to address business opportunities that they could not undertake individually”³. In other words, it is a temporary alliance of (usually small and medium sized) enterprises that join together to share skills or core competencies and resources in order to better respond to business opportunities, and whose cooperation is supported by computer and communication networks⁴. Thus a VE can be considered as a weakly-connected system where participants define their actions independently in order to achieve a common goal⁵, and participant cooperation is supported by computer networks^{6, 7, 8}. Moreover, when the business opportunity terminates, the units leave the network and give rise to new forms of organizations.

The main obstacles to the development of VEs have been identified in the limits of their supporting cooperation platforms, and in the inefficiency of their organizational configurations. Furthermore, there is a lack of mechanisms aimed to increase trust and security in these online settings^{9, 10}. More generally, a critical element in the implementation process of inter-organizational systems is represented by the identification of information to be shared and their quality characteristics. Among these characteristics, information security plays a crucial role as the enabler of trust^{11, 12, 13}, which is particularly needed when ownership relations among partners are lacking, and a strong integration is required^{14, 15, 16, 17, 18}. In particular, we refer here to the concept of “systemic trust” which has been introduced by Sztompka¹⁹ as the combination of institutional, technological and commercial trust.

Previous conceptual works have focused on the role of federated identity management systems as trust-reinforcing mechanisms when multiple organizations need to cooperate^{12, 20, 21}. These security solutions are based on a combination of several technical, administrative, and informal aspects in order to ensure the expected benefits⁹. They represent an alternative to the most common centralized architectures which pose a number of issues when access control is needed across organizational boundaries.

In this paper, we aim to explore the characteristics of trust-reinforcing mechanisms in the context of virtual enterprises. Furthermore, we aim to understand to what extent federated identity management systems represent

a suitable solution to security issues in this domain. Our empirical analysis is based on a case study²² performed on a research project (LD-CAST) for the development of a cooperation framework supporting the provision of cross-border e-services.

The LD-CAST (Local Development Cooperation Action Enabled by Semantic Technology) project has been funded by the European Commission by involving as service providers the Chambers of Commerce from four different countries, and as members of the consortium, one university, two research centers and three IT system integrators. The ultimate goal of the research project has been to define a cooperation framework, and to develop a prototype of the supporting semantic platform. Both types of results have been validated in the last phase of the project, and they were approved by the EU Commission in 2008. For the purposes of this paper, we refer to data collected during the 30 months of the project in the form of official documents, meeting minutes, interviews, and direct observations. In fact, both authors have been directly involved in project activities.

In the following sections we first outline the LD-CAST platform non-functional requirements, which address security issues. Then, we provide an overview of the choices that have been made in the design of the platform architecture, with a particular reference to the federated identity management subsystem. Finally, we suggest possible generalization of our findings together with implications for research and practice.

2. SECURITY ISSUES AND NON-FUNCTIONAL REQUIREMENTS

Before detailing the non-functional requirements identified in the LD-CAST project, we briefly introduce the security issues that have emerged during the project. In order to present these requirements, we refer to the ISO 17799 standard which is widely recognized as a de facto standard for describing good practices in information security processing^{23, 24}. This standard enlists the various aspects that must be taken into account for managing information systems security, and organizations are requested to select the controls that fit with their security needs. By referring to the area of “Access control”, a set of 7 objectives and 25 controls are described in the standard. Among these, the following objectives have been considered as applicable to the LD-CAST platform by the project consortium:

- Business requirements for access control: user’s access to information, and to business processes should be controlled on the basis of business

and security requirements. This should take into account policies for information dissemination and authorization.

- User access management: formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users, to the final de-registration of users who no longer require access to information systems and services.
- Network access control: access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring: appropriate interfaces between the organization's network and networks owned by other organizations, or public networks; appropriate authentication mechanisms for users and equipment; and, control of user access to information services.

2.1 LD-CAST Non-Functional Requirements

In the LD-CAST case, the above-mentioned objectives have been translated in the requirements and therefore in procedural and architectural design choices. The first objective (business requirements for access control) can be achieved through a formal agreement among partners and through a set of authorization rules defined by each member providing services or information. The second objective (user access management) asks for a set of formal procedures, and a technical system to manage user credentials. This can be achieved using a centralized or a decentralized approach, depending on the system architecture. Finally, the third objective (network access control) asks for a set of mechanisms to control user access to the network. In this case, a decentralized approach presents the advantage of leaving the choice of an appropriate technical solution for access control and monitoring to each identity provider. With these premises, the following non functional requirements have been defined for the LD-CAST platform: i) identity management requirements: since legal issues arise in centralizing information about users, a decentralized approach for the management of user's data is required; ii) identification requirements: different mechanisms (i.e. digital certificates, smart card, certified e-mail message or face-to-face) are accepted to complete the registration phase, by different Local Agencies (i.e. Chambers of Commerce). Each Local Agency should be in charge of the identification of its own registered users; iii) authentication requirements: a Single-Sign-On mechanism should be provided to users accessing the overall LD-CAST system. Authentication should be based on username and

password; iv) authorization mechanism: depending on the rules and policies of each service provider, an authorization mechanism for executing services and activities should be defined.

Discussion among LD-CAST partners has led to the decision of adopting a federated identity management system. This technology has been seen as an alternative to the most common centralized solutions supporting the online cooperation of different organizations. Moreover, in order to also satisfy compliance requirements with privacy regulations, project partners have also investigated innovative solutions by analyzing and comparing the results of other recent EU-funded research projects (i.e. FIDIS, PRIME, etc.). Therefore, the choice of implementing a federated identity management system has been made also in accordance with this additional requirement.

3. IDENTITY MANAGEMENT SOLUTIONS

Before describing how the above-mentioned requirements have influenced the LD-CAST architectural choices, we introduce the main characteristics of federated identity management systems. In the context of identity management systems, the term “subject” refers to an entity, typically a user or a device, which needs to authenticate itself in order to be allowed to access a resource. Subjects then interact with authentication systems of various types at various sources. An authentication type is the method the subject uses to authenticate itself (i.e. by providing user ID and password). An authentication source is the authority that controls the authentication data and protocol. Authentication takes place both within an organization, and among multiple organizations. Even within an organization, there may be multiple sources. However, traditional authentication systems generally presume a single authentication source and type. An example is given by Kerberos²⁵, in which the source is a trusted Key Distribution Center (KDC) and the type is user IDs with passwords. In a Public Key Infrastructure (PKI), the source is the Certification Authority (CA) and the type is challenge/response. While both Kerberos and PKI permit multiple authentication sources, these authentication sources must be closely coupled. Often, complex trust relationships must be established and maintained among the sources of authentication. This can lead to authentication solutions that are operationally infeasible and economically cost-prohibitive.

A practical view of inter-organizational communications reveals that having a single type of authentication is a rare possibility. In fact, the involved organizations will be supporting multiple authentication types,

such as passwords, tokens, certificates, and smart cards. Therefore, security architectures should include a single infrastructure for managing all of these types, rather than a separate infrastructure for each of them. In this practical model, the many authentication sources form a federation, where each member of the federation can ascertain the authenticity of a set of subjects.

In this context, the term “federated” refers to multiple authentication types and sources. The pre-condition for the implementation of a federated identity management system is the existence of a “circle of trust”, defined as a group of organizations that have established trusted relationships and have pertinent agreements in place regarding how to interact with each other, and how to manage user identities. Once a subject has been authenticated by an identity provider within a circle of trust, this subject will be easily recognized by the other service providers within the same circle of trust.

3.1 The Ld-Cast Architecture

During the design phase of the LD-CAST project, the Liberty Alliance project was identified as a possible answer to the above-mentioned requirements. The Liberty Alliance project was aimed to foster the development of standards and specifications for federated identity systems. For example, the Liberty specifications provide mechanisms for single sign-on, and for linking separate accounts within a group of service providers in a circle of trust.

Such an architecture allows users to sign in only one time during the session, and it enables interactions with any service provider or identity provider in the circle of trust without any other login operation until the next logout. Moreover, the user’s registration data are gathered only by the identity provider chosen by each user, with obvious advantages in terms of privacy concerns.

Hence, in the LD-CAST case this federated identity management architecture has been implemented by considering that the final user (i.e. the entrepreneur) interacts with service providers (i.e. a foreign Chamber of Commerce) by performing the authentication process with his/her own identity provider (i.e. the local Chamber of Commerce to which s/he is registered). All of these interactions are made possible by the agreement among all the actors involved that become members of the above-mentioned circle of trust.

4. DISCUSSION AND CONCLUSIONS

Organizations around the world protect access to sensitive or important information through the use of access control rules. In every electronic transaction context, such as in the LD-CAST case, identity management solutions play a key role within the mechanisms for reinforcing trust. In this paper we have shown that federated identity management systems represent a possible architectural solution to change the way consumers, businesses, and the government performs online authentication and authorization. The LD-CAST case confirms the hypothesis that federated identity management systems fit with non-functional requirements related to security issues. In fact, the above-mentioned concept of circle of trust and the Liberty Alliance architectural specifications also seem to fit well with the LD-CAST non-functional requirements. In particular, this architectural solution allows to tightly couple together the three basic interactions between the user, his or her identity provider (i.e. the local Chamber of Commerce), and a generic service provider, during the authentication and authorization process. These three basic interactions are i) the user authentication; ii) the access request; and, iii) the delivery of authorization attributes from the identity provider towards the service provider.

According with the case study research strategy, the main contribution of this study is based on the possibility to analytically generalize the LD-CAST findings. In fact, the group of local agencies providing cross-border G2B e-services through the LD-CAST platform can be considered as an instantiation of a virtual enterprise, whereas identity management systems represent an instantiation of a trust-reinforcing mechanism. Federated identity management systems have confirmed their role as a possible alternative to the most commonly centralized solutions when supporting the online cooperation of multiple organizations. Furthermore, the LD-CAST non-functional requirements can be generalized in order to derive access control requirements for IT systems supporting virtual enterprises. These contributions have several implications for practitioners involved in the design of such IT systems.

However, since the LD-CAST project goal was to provide a proof of concept of the implemented technological solution, our data do not include any information on the real behavior of the virtual enterprise. At the same time, this represents a limitation of our work, and an opportunity for further research in this field. Moreover, since the relationship between network behavior, security and trust goes beyond the scope of the present paper, we also consider this as a possible direction for developing future investigations in this domain through empirical studies and simulation models^{26, 27}.

5. REFERENCES

- [1] P. Spagnoletti, and S. Za, A design theory for e-Service environments: The interoperability challenge. In M. Snene (Ed.), *Exploring Services Science* (p201-211). Heidelberg: Springer-Verlag, 2012. http://dx.doi.org/10.1007/978-3-642-28227-0_15.
- [2] A. D'Atri, Organizing and managing virtual enterprises: The ECB Framework. In L.M. Camarinha-Matos, and H. Afsarmanesh (Eds.) *Processes and Foundations for Virtual Organizations* (p171-178). Boston: Kluwer Academic Publishers, 2003. http://dx.doi.org/10.1007/978-0-387-35704-1_18.
- [3] H. Gou, B. Huang, W. Liu, and X. Li, A framework for virtual enterprise operation management. *Computers in Industry*, 50(3), p333-352, 2003. [http://dx.doi.org/10.1016/S0166-3615\(03\)00021-6](http://dx.doi.org/10.1016/S0166-3615(03)00021-6).
- [4] P. Depaoli, and S. Za, Towards the redesign of e-Business maturity models for SMEs. In R. Baskerville, M. De Marco, and P. Spagnoletti (Eds.), *Designing Organizational Systems* (p285-300). Berlin, Heidelberg: Springer, 2013. http://dx.doi.org/10.1007/978-3-642-33371-2_15.
- [5] C.F. Bremer, W. Eversheim, M. Walz, and A.M. Gutierrez, Global virtual business: A systematic approach for exploiting business opportunities in dynamic markets. *International Journal of Agile Manufacturing*, 2(1), p1-11, 1999.
- [6] N. Wu, and P. Su, Selection of partners in virtual enterprise paradigm. *Robotics and Computer-Integrated Manufacturing*, 21(2), p119-131, 2005. <http://dx.doi.org/10.1016/j.rcim.2004.05.006>.
- [7] A. Motro, A. D'Atri, A. Brodsky, and N.E. Egge, Optimizing procurement decisions in virtual enterprises. *International Journal of Decision Support System Technology*, 4(3), p43-67, 2012. <http://dx.doi.org/10.4018/jdsst.2012070104>.
- [8] A. Motro, and Y. Guo, SOAVE platform: A service oriented architecture for virtual enterprises. In L.M. Camarinha-Matos, L. Xu, and H. Afsarmanesh (Eds.), *Collaborative Networks in the Internet of Services* (p216-224). Berlin, Heidelberg: Springer, 2012. http://dx.doi.org/10.1007/978-3-642-32775-9_22.
- [9] R. Åhlfeldt, P. Spagnoletti, and G. Sindre, Improving the information security model by using TFI. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R.V. Solms (Eds.), *New Approaches for Security, Privacy and Trust in Complex Environments* (p73-84). Boston: Springer, 2007. http://dx.doi.org/10.1007/978-0-387-72367-9_7.
- [10] P. Spagnoletti, and A. Resca, A design theory for IT supporting online communities. In R.H. Sprague (Ed.), *Proceedings of the 45th Hawaii International Conference on System Sciences* (p4082-4091). Los Alamitos, California: IEEE Computer Society Press, 2012. <http://dx.doi.org/10.1109/HICSS.2012.54>.

- [11] M. Cavallari, Information systems security and end-user consciousness - A strategic matter. In A. D'Atri, M. De Marco, A.M. Braccini, and F. Cabiddu (Eds.), *Management of the Interconnected World* (p251-258). Berlin, Heidelberg: Physica-Verlag HD, 2010. http://dx.doi.org/10.1007/978-3-7908-2404-9_29.
- [12] P. Spagnoletti, S. Za, and A. D'Atri, Institutional trust and security, new boundaries for virtual enterprises. In L. Kutvonen, P. Linington, J.-H. Morin, and S. Ruohomaa (Eds.), *Proceedings of 2nd International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems. Helsinki University Printing House, HELSINKI—FIN* (p67-78). Helsinki: Helsinki University Printing House, 2007.
- [13] S. Za, E. D'Atri, and A. Resca, Single sign-on in cloud computing scenarios: A research proposal. In A. D'Atri, M. Ferrara, J.F. George, and P. Spagnoletti (Eds.), *Information Technology and Innovation Trends in Organizations* (p45-52). Berlin, Heidelberg: Physica-Verlag HD, 2011. http://dx.doi.org/10.1007/978-3-7908-2632-6_6.
- [14] R. Bachmann, and A.C. Inkpen, Understanding institutional-based trust building processes in inter-organizational relationships. *Organization Studies*, 32(2), p281-301, 2011. <http://dx.doi.org/10.1177/0170840610397477>.
- [15] W. Ford, and M. Baum, *Secure electronic commerce*. Upper Saddle River, NJ, USA: Prentice Hall, 1997.
- [16] D. McKnight, L. Cummings, and N. Chervany, Initial trust formation in new organizational relationships. *Academy of Management Review*, 23(3), p473-490, 1998. <http://dx.doi.org/10.2307/259290>.
- [17] P. Pavlou, H. Liang, and Y. Xue, Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *Mis Quarterly*, 31(1), p105-136, 2007.
- [18] S. Ray, T. Ow, and S.S. Kim, Security assurance: How online service providers can influence security control perceptions and gain trust. *Decision Sciences*, 42(2), p391-412, 2011. <http://dx.doi.org/10.1111/j.1540-5915.2011.00316.x>.
- [19] P. Sztompka, *Trust: A sociological theory*. Cambridge: Cambridge University Press, 1999.
- [20] C. Schlaeger, and G. Pernul, Authentication and authorisation infrastructures in B2C e-Commerce. In K. Bauknecht, B. Pröll, and H. Werthner (Eds.), *E-Commerce and Web Technologies* (p306-315). Berlin, Heidelberg: Springer, 2005. http://dx.doi.org/10.1007/11545163_31.
- [21] M. Olden, and S. Za, Biometric authentication and authorization infrastructures in trusted intra-organizational relationships. In A. D'Atri, M. De Marco, A.M. Braccini, and F. Cabiddu (Eds.),

- Management of the Interconnected World* (p53-60). Berlin, Heidelberg: Physica-Verlag HD, 2010. http://dx.doi.org/10.1007/978-3-7908-2404-9_7.
- [22] R.K. Yin, *Case study research: Design and methods*. Thousand Oaks: Sage Publications, 2003.
- [23] ISO/IEC, *ISO/IEC 17799: Information technology- Security techniques - Code of practice for information security management*. Geneva: International Standards Organization, 2005.
- [24] P. Spagnoletti, and A. Resca, The duality of Information Security Management: Fighting against predictable and unpredictable threats. *Journal of Information System Security*, 4(3), p46-62, 2008.
- [25] J. Kohl, and C. Neuman, *Kerberos network authentication service (V5)*. United States: RFC Editor, 1993.
- [26] S. Za, and P. Spagnoletti, Knowledge creation processes in information systems and management: Lessons from simulation studies. In P. spagnoletti (Ed.), *Organizational Change and Information Systems* (p191-204). Berlin, Heidelberg: Springer, 2013. http://dx.doi.org/10.1007/978-3-642-37228-5_19.
- [27] F. Marzo, S. Za, and P. Spagnoletti, Modeling dependence networks for agent based simulation of online and offline communities. *Lecture Notes in Artificial Intelligence*, 7879, p192-203, 2013. http://dx.doi.org/10.1007/978-3-642-38073-0_17.