Solving Identity Management and Interoperability Problems at Pan-European Level

Sergio Sánchez García and Ana Gómez Oliva

DIATEL – Universidad Politécnica de Madrid,
Ctra. Valencia Km.7, 28031, Madrid, Spain
{sergio, agomez}@diatel.upm.es

Abstract. In a globalized digital world, it is essential for persons and entities to have a recognized and unambiguous electronic identity that allows them to communicate with one another. The management of this identity by public administrations is an important challenge that becomes even more crucial when interoperability among public administrations of different countries becomes necessary, as persons and entities have different credentials depending on their own national legal frameworks. More specifically, different credentials and legal frameworks cause interoperability problems that prevent reliable access to public services in a cross-border scenarios like today's European Union. Work in this doctoral thesis try to analyze the problem in a carefully detailed manner by studying existing proposals (basically in Europe), proposing improvements in defined architectures and performing practical work to test the viability of solutions. Moreover, this thesis will also address the long-standing security problem of identity delegation, which is especially important in complex and heterogeneous service delivery environments like those mentioned above. This is a position paper.

Keywords: eIdentity, identity federation, identity delegation, interoperability.

1 Introduction

Many European countries have traditionally used a universal system of identification based on a single document that is provided to all individuals. The content and function of the document are broadly similar in all cases, as it is normally used as a method for identifying individuals in dealings with either public administrations or some private companies who need to identify users of their services. Given that the document reflects a person's identity, civil servants or company employees can directly verify someone's identity on sight. Nevertheless, Internet and the gradual incorporation of the public to the digital society have led to changes in this scenario, as ever more administrative processes in both public institutions and service providers are being conducted online. Therefore, a growing demand exists for systems of identification that can enable such transactions without a loss of guarantees in the terms of security. This has given rise to the need to provide the public with an *electronic* or *digital identity* that will allow people to identify themselves online with at least the same guarantees as with a public identity card in personal interactions.

R. Meersman, P. Herrero, and T. Dillon (Eds.): OTM 2009 Workshops, LNCS 5872, pp. 805–809, 2009.

With a view to solving this problem, most countries in the European Union are engaged in the implementing of electronic identification cards or *eID cards* whose outward appearance is similar to present-day identification cards, except that it includes a chip. This chip can electronically store information on identity and enables interaction with certain validation applications, thus allowing users to digitally prove their identity. Europeans are living in an environment that is not only increasingly digitalized, but which is increasingly globalized. Today, a citizen of Spain can work for a German company and perform his or her work in Belgium and do so problem-free, in theory; such a person must be able to interact with the company and with different public administrations online. This global environment leads to a series of problems that arise when we ask questions like the following: How could a person with a Spanish electronic identification card access online services provided by German public administration? And what about the person's employment data as a worker in Belgium? Further, how can German public institutions manage the identity data of the Spanish national?

2 Material and Related Work

Answers to the questions posed above are no simple matter; in any event, these will involve the specification and development of a set of technical and organizational infrastructures that can define, administer and manage attributes related to the identity of individuals. These infrastructures are called *Identity Management systems,* or IDMs. On the basis of action plans launched by the European Union, in recent years a number of initiatives have focused on achieving pan-European interoperability between identity management systems. Although most of these initiatives are nothing more than theoretical proposals that solve some problems without providing a comprehensive solution, some do go further and propose architectures that are now in the pilot stage. Coupled with standards and proposals such as SAML (*Security Assertion Markup Language*), WS-* (*Web Services standards and recommendations*) or Liberty, these proposals constitute the base material for a study of both the present state of affairs and for work related to the subject of this paper; further, they will be used to formulate the set of hypotheses that will guide continuing research work. Therefore, a brief analysis follows of the most outstanding of these proposals.

One of the first studies or projects related to interoperability of identity management systems was the Modinis eIDM Study [1], which studied the use of electronic identity management systems in the European Union and analyzed the most significant consequences of using these eIDM systems. The study's main contribution to interoperability was its definition of a model or conceptual framework (the Modinis Conceptual Framework), which is essentially a federation-based portal that incorporates the key proposals made in the project on the general organization and basic principles that should govern eIDM infrastructure at a pan-European level. It is based on a federated model that relies on a series of identity portals in each Member State responsible for authenticating entities at a national level and deciding the trust level granted to authentication processes in another Member State, so that each State will accept as equivalents the authentication levels and mechanisms used in another State on the basis of a set of criteria, while no specific Europe-wide infrastructure would be required.

Another interesting system is the TLS-Federation [2]. This project aimed at providing a regulatory and interoperable working framework for identity management at a pan-European level. It focused on employing technologies and standards that were sufficiently well-known and on protecting of the user side against possible scenarios of identity theft. The system is based on the use of certificates during the authentication process and is built upon a user-centered approach in which identity and privacy attributes are directly managed by the user. It is the only solution that requires no, or very little additional installation, and it does not demand conversion of session credentials in online access from the domain of any Member State within the pan-European domain.

The GUIDE project (*Creating a European Identity Management Architecture for eGovernment*) [3] sought to develop a model for identity interoperability within the European Union, so as to enable Member States to trust the identity of an entity – whether individuals or companies – in another State. The underlying concept involves a federated network of identity management in which members, users, institutions and companies throughout the European Union can participate in identity information exchanges without compromising the privacy or security of the information. It requires membership in circles of trust based on operational agreements, thus yielding a federation of service providers and identity providers. Many Member States are involved in the development of such federations at a national level but they are often being created in isolation from one another. The objective of GUIDE was to define an architecture to enable the joining of these federations into a large circle of trust with a view to creating a single identity environment throughout the European Union.

Another proposal for a pan-European identity management system is STORK (*Secure idenTity acrOss boRders linKed*) [4]. This recently-begun project seeks to develop and test common specifications for mutual and secure recognition of national electronic identities (eID) of participating countries. Their specific objectives include defining common models and specifications for the mutual recognition of eIDs between countries, verifying in a real environment easy and secure eID solutions to be used by individuals and companies and achieving coordination with other initiatives of the European Union in order to maximize the usefulness of eID services. To do this, they propose a model based on preliminary studies conducted by IDABC (*Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*) [5] that describe, at a high level, a federated model for interoperability that is technologically neutral and which supports multiple levels of authentication.

3 Research Hypotheses

Having discussed the identity management systems that might be considered the most significant at a pan-European level, an overall assessment can be made of them and a series of conclusions drawn as the basis for a hypotheses upon which a thesis could be formulated.

Out of all the models presented, it would seem rational to assume that the path to follow would lead to a system based on federation and multi-level operation. Indeed, all the systems discussed herein have a federated infrastructure that can separate

provision of the service from processes related to digital identity that are necessary to provide said service – i.e., user registration, generation and storage of identity and authentication data. The fact that the system is multi-level also facilitates, a priori, the incorporation of all countries with digital identity and an identity management system, thus speeding up the implementation of the system. Another aspect to be underlined that is common to MODINIS [1], IDABC [5] and STORK [4] is the meager or non-existent need to deploy a pan-European infrastructure and their capacity to quickly and easily add to the system countries that are less developed or which have fewer resources. Due consideration must also be given to the use of standards that have been sufficiently tested and accepted, if possible, as with TLS in the TLS-Federation model.

With respect to outstanding problems that require a solution, that of trust is perhaps the most important. Specifically, trust levels must be established that will allow users with a certain type of identity tokens from their own country to be authenticated at a global level, but also with equivalences and trust levels in authentications. Consequently, authorization levels could be established in access to service providers by member states in the federated identity network.

Another issue to be solved is semantic interoperability, which is closely linked to multilevel operability. Incorporation within a pan-European system of solutions that have already been implemented at a national level demands translation between representation formats at interconnection points, which also implies a need to establish a certain degree of semantic interoperability.

Finally, although no less important, there is the problem of identity delegation and authorization. Many transactions today are performed by legal representatives who are authorized to act on our behalf. For example, an individual in Spain can authorize another person to engage in all transactions necessary to file an income tax return with the authorities. Likewise, a person can have different roles simultaneously within the identity management system, acting as both an individual and the legal representative of a company or organization; that is, the identity of a person or entity can be delegated to another, thus empowering the latter person to act, to all intents and purposes, as if he or she were the former person or entity. Since none of the proposals discussed herein even address this issue, none of them offer a solution to it.

4 Work Planned

On the basis of the hypotheses formulated, future work on the thesis will primarily seek to solve two of the problems found: first, the problem related to interoperability in environments of multi-level authentication arising from the need for a translation mechanism; and, secondly, the problem of delegation. For the latter case, thesis work will endeavor to propose a global solution for delegation that is both secure and sufficiently flexible to adapt to any architectures that should arise in the future.

In addition, solutions will also be sought for problems found in the architectures proposed to date. Thorough follow-up will also be performed on proposals in progress such as STORK [4], attempting to provide, to the extent possible, solutions to any problems that may be identified. Given that this thesis work is being carried out in the framework of a national project (TSI2006-4864 *Plataforma telemática de*

Administración Electrónica basada en coreografía de servicios [Telematic platform of electronic government based on a choreography of services]) validation is available on a small scale for testing, in a real city council, the viability of the solutions proposed.

5 Conclusions

Today, pan-European identity management in public administrations has become a major challenge to which a solution has not yet been found. Even though proposals exist, none of them constitute a complete and fully validated solution. Upcoming work on this thesis will endeavor to provide an in-depth study of solutions conceived to date, comparing them, identifying problems and supplying solutions both to problems found and problems not addressed – as in the case of delegation -, with a view to allowing the results to be given their proper weight when a pan-European identity management system is adopted.

Acknowledgments. This thesis is part of the work being conducted by the research group T>SIC, to which the authors herein belong, as part of the project TSI2006-4864 *Plataforma telemática de Administración Electrónica basada en coreografía de servicios* [Telematic platform of electronic government based on a choreography of services], which is supported by the Spanish Ministry of Education and Science under the national R+D+I plan.

References

1. ModinisIDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome
2. Bruegger, B.P., Hühnlein, D., Schwenk, J.: TLS-Federation - a Secure and Relying-Party-Friendly Approach for Federated Identity Management, http://porvoo14.dvla.gov.uk/documents/tls_federation_final.pdf
3. GUIDE, Creating a European Identity Management Architecture for eGovernment, http://istrg.som.surrey.ac.uk/projects/guide/overview.html
4. STORK, Secure idenTity acrOss boRders linked, http://www.eid-stork.eu/
5. Majava, J., Graux, H.: Common Specifications for eID interoperability in the eGovernment context. IDABC European eGovernment Services (December 2007), http://ec.europa.eu/idabc/servlets/Doc?id=30989