Privacy and Capability Management for the European eIDM Framework

Mario Reyes[1], Ignacio Alamillo[2] and Daniel Chavarri[1]

[1] S21sec Labs, Parque empresarial La Muga, Nº11, Planta 1, Oficinas 1 - 6, 31160 Orcoyen, Spain.
[2] Agència Catalana de Certificació, Passatge de la Concepció, 11 08008 Barcelona, Spain

Abstract. The natural evolution of eGovernment is to go beyond the management of identities and therefore it is necessary to manage people, companies or organizations, and their capabilities to interact with Public Administrations. When developing an application based on an eID management system, this management issue must be tackled within each application (i.e. demonstrate the capability of one person to act, demonstrate the economical reliability, demonstrate his professional status, etc ...) and is normally based on the local jurisdiction. The objective of the present paper is to introduce a distributed system for the privacy-enhanced management of the capabilities associated to a person within the EU framework, independently from the origin and destination EU member state. The core of this system is the intelligence of the Capabilities Resolution Nodes (CRN) to cope with the complexity of the capability resolution and the capability sources discovery in the pan-European scenario. A European Capacity Resolution Network will be able to grow up the interoperability of the digital identities provided and valid in each member state and will answer the question "is this person, identified with this digital identity and who is described by those attributes, allowed to carry out this legal act in this country according to its law?".

Keywords: privacy-enhanced tools, attribute management, legal roles, ontologies, semantic web, electronic government, identity management, interoperability

1 Introduction

In today's Europe citizens are free to work and re-locate within the Union. Enterprises trade and carry out business across the Union. When citizens and enterprises do this they frequently have to interact with national public administrations. Member States are currently putting in place eGovernment[1] strategies that will allow such

[1] EGovernment seeks to use information and communications technologies to improve the quality and accessibility of public services. It can reduce costs for businesses and administrations alike, and facilitate transactions between administrators and citizens. It also

interactions to take place electronically. In parallel, they are frequently improving their business processes and the way in which business with citizens and enterprises is carried out. However, *there is a risk that that the development of government e-services may inadvertently result in the erection of barriers* to the continued development of the single market and the associated freedoms of movement. This would happen if citizens and enterprises that need to interact electronically with a national public administration other than their own were unable do so. For enterprises it could mean a relative loss of competitiveness, and for citizens increased costs. For Europe it could mean that the development of the single market and the associated four freedoms is hampered or even blocked.

Full-scale implementation of eGovernment raises difficult issues. These include:

- Safeguarding trust and confidence in on-line interaction with governments,
- Widespread access to on-line services so that no digital divide is created,
- Interoperability for information exchange across organizational and national borders,
  - *organizational* nature, which affect the processes and the *collaboration* between the administrations;
  - *semantic* nature, which is not limited to the interconnectivity of information resources, but also extends to the area where information can be *interpretable* by automatic and consequently *re-usable* forms of software applications that did not take part in the information resources' creation;
  - *technical* nature, which is the most direct form of *interconnection* of applications through diverse technological components; in particular, the development and ubiquity of the Internet technologies, on the base of *standards* and *open specifications* that are universally accepted have allowed for a high degree of technical interoperability.
- Advancing pan-European services that support mobility in the Internal Market and European Citizenship.

In this context, privacy laws impose strict controls on the interchange of personal information, an issue which is specially delicate when the information to interchange is identity information or, in our case, capabilities information, such as authorizations, delegations, powers of attorney and the representation of minors or incapables

1.1 The current scenario for capabilities management

When developing an application (business application, public procurement application ...) based on an eID management system, each application must develop the capability logics (i.e. demonstrate the capability of one person to act, demonstrate the economical reliability, demonstrate his professional status, etc ...), logic which is usually connected to legal theory in a concrete local jurisdiction. The present reality is

---

helps to make the public sector more open and transparent and governments more understandable and accountable to citizens.

that we negotiate the connection with the information sources locally in personalized scenarios and manage these “attributes” inside that application. Each change in the applied philosophy or in regulations implies the re-development of the application to adapt it to these new environmental conditions, even if the final logic of the application has not changed at all.

Moreover, when we are facing a pan-European or wider scenario, the complexity to build an application intelligent enough to deal with other ID attributes and information sources is enormous (who hosts that info? How can it be provided? How to understand and manage the relevant information?,...). Furthermore there are potential legal issues to be solved: roles and mandates are not homogeneous throughout Europe, privacy laws must be respected in both member states and so forth.

As an example, in a current real e-procurement scenario, if a company want to access a public procurement process in another member state, the representative will be able to identify himself (with current Identity Management technology/infrastructure) but his capability to act as a representative of that company has to be proved also ;… perhaps he will be able to do it locally (in his member state identity), but when trying to solve this for another member state he will be asked for registration of his capability to act as a representative in the destination member ’s state system. …The conclusion is that he will have to go through all the physical procedures in the destination member state to be inscribed as a potential user of the system The normal situation nowadays is that every company must be inscribed in on-line registers (registration that must comply with national laws and thus must be done locally) in every member state (27 times the same procedure).

The actual research challenge should not be aimed towards the integration and deployment of the identity management technologies that are currently in the standardization process, but it should be a step further, focusing on the real-world management of identity management contents (capabilities resolution) and the use of people management contents.

Moreover, it is of paramount importance to consider the privacy issue, as law requires that personal identifiable information must be under control of its owner. Some of the current proposed models of eGovernment initiatives do no consider the citizen as an active actor of the system, but just as an object about which different Public Administrations interchange data: these models present some potential deficiencies to comply with the privacy laws, and as a consequence may not be fully applied to the capabilities resolution domain.

On the contrary, the model we propose do consider the citizen as the actor that controls the capability information that she wants to share with one or more Public Administrations, in her local jurisdictions or along the network.

2 The proposed system

The main objective of the research work is the creation of a distributed system for the management of the capabilities associated to a person (a person is a set of one or more identities) within the EU framework independently from the origin and destination EU member state. This platform will integrate an intelligent system for arbitrating and routing the process flow needed for the capabilities resolution.

The solution is an intelligent system that releases the final application from the complex logic associated with the capability management in a pan-European framework. This simplifies the creation of the final application for businesses and eGovernment applications and at the same time will allow end users (EU citizens) to not only identify themselves in all member states (nowadays this is a fact) but also to be able to act in other member states. Moreover, the system will be a key tool for the citizen to be able to control the attributes and capabilities associated to his set of identities, which is a sound strategy to comply with privacy regulations and to generate user confidence.

The platform will allow any EU citizen in any EU member state to perform private and public procedures, whilst the capabilities resolution will take place in the credentials' origin country if the user has agreed to such a use of his identities. The result will be a real teleprocessing of administrative procedures in the EU framework. Moreover, the system will comply with the legislative framework in the field of privacy of personal data in each EU member state, as the information will not flow through the network without explicit user consent. Each origin member state will resolve the capabilities of a user in the same member state. This approach will follow the EC eGovernment Unit Roadmap design criteria, which state that the pan-European eIDM system must be 'federated in a policy sense'; in other words, this means that administrations mutually trust each other's identification and authentication methods, on the basis that they were considered acceptable by the originating administration.

At this stage of the research, the Catalan Certification Agency is leading the development of a platform for the management of capabilities in Catalonia, called Project PASSI, with the full set of functionality but limited in the scope to the Spanish law. At the moment, the first set of connectors are being developed, to allow a citizen to acquire and share her capabilities registered by Notaries (powers of voluntary representation) with the Catalan Public Administrations adhered to the system, using the interconnection infrastructure offered by the public administrations consortium AOC.

2.1 The proposed architecture

The system proposed does not consist in the network itself (that will follow a federated model and will be based on previous research work) but on the intelligence of the Capabilities Resolution Nodes (CRN) to cope with the complexity of the

capability resolution and the capability sources discovery in the pan-European scenario (figure 1).

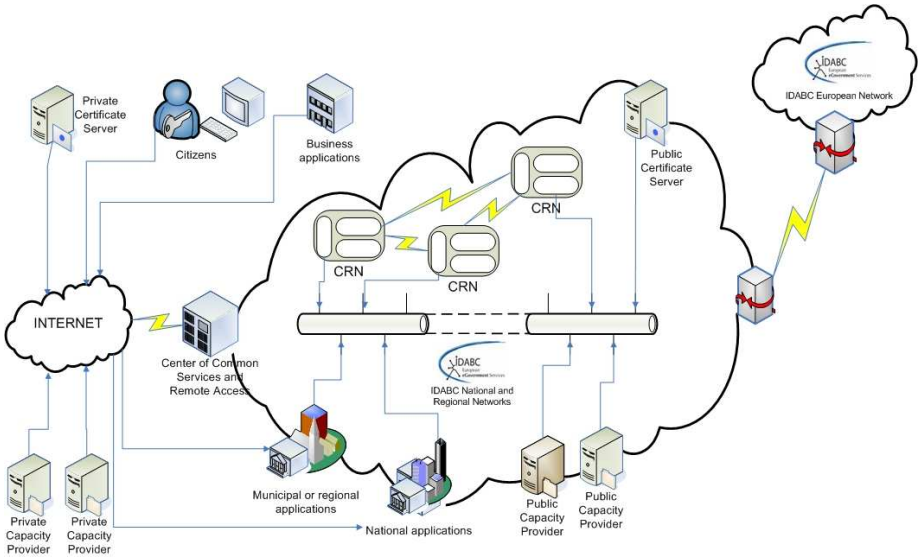

Figure 1. Local Domain: citizen access to the services of the public administration; then, the application of the administration accesses the CRN through the infrastructure of the National and Regional networks.

For this purpose the following modules are developed:

- A **semantic model** to provide the necessary knowledge for the resolution of capabilities. The system should be capable of addressing the appropriate capabilities provider for the resolution of a specific capability.
- An **expert system** that will learn how to resolve the capabilities for a specific purpose, using machine learning technologies and intelligent agents.
- A **conceptual taxonomy** service able to map between roles and procedures in different domains (European, national, regional, local).
- **Interfaces** for the management, administration and communication between the platform providers, both service providers, identity providers and capacity providers. Similarly they are had to include the interfaces necessary to integrate the CRNs in the TESTA network.

2.2 Standards and related work

The Project relies on current Identity Management Technologies, most of which are in the process of being standardized:

- The XACML standard for resources access control, modified in order to include the capability resolution and to allow this resolution to be made in a distributed way.
- The SAML standard as a base to request identity and attribute information related to a given user.
- The Liberty Alliance standard, further analyzed to define the trust and security model for the capabilities federation.
- The federation concept becomes crucial to the concepts of association of identities and pan-European networks of identities. Only in this form is the citizen able to efficiently manage his personal character data.
- The platform is SOA based. Research is needed in this field for the definition and study of the workflows for the presented scenario, establishing a set of recommendations in the web services development phases for the public administrations.

3 Conclusion

The major contribution will not be Identity Management, but the capability and content management associated to an identity in an EU framework.

- **Ontology and semantics** are able to provide knowledge to the building blocks of the distributed intelligent manager. This is the main research block as, on the one hand it is mandatory to represent the semantic models of the member states laws as well as the EU directives, and on the other hand these models must represent the semantic relationship between all the EU legislation.
- The capability resolution intelligent manager will include the **logic required to increase its knowledge** while it continues resolving the assigned tasks (intelligent agents and machine learning). It must be capable of discovering where to direct its consultation to, so that a certain capacity is resolved.
- **Information security** in every area: access, authorization, information flow, personal data protection, citizen rights and audit. The recommendations coming from this project will be valid for the small administration as well as for large corporative administrations; different recommendation levels will be used to address all relevant stakeholders.
- The resulting system is a **privacy enhancing tool** (PET) in which the end user can manage his identities, his information, his personal character data, knowing at any moment where these data are and who has access to them. Furthermore, the provision of explicit access control to identity data by the user. As a consequence, the end user is able to share and to control the use of his attributes and consequently his capabilities.

References

1. Ignacio Alamillo, Xavier Urios: La Gestión de identidades y capacidades por las administraciones públicas. TECNIMAP. Sevilla (2006).
2. Ignacio Alamillo: Beyond identity management: capabilities management as a Public Administration simplification technique.
3. Consultation document for a future policy paper on pan-European Government e-Services. http://ec.europa.eu/enterprise/consultations/government_e-services/
4. IDABC, European eGovernment Services. http://ec.europa.eu/idabc/
5. TESTA: Trans European Services for Telematics between Administrations. http://ec.europa.eu/idabc/en/document/2097/
6. Torsten Priebe, Wolfgang Dobmeier, Nora Kamprath: Supporting Attribute-based Access Control with Ontologies. ARES 2006: 465-472
7. Kamelia Stefanova, Dorina Kabakchieva: User involvement in identity management e-Government architecture Development. Proceedings from workshop on User Involvement in e-Government development projects. September 12, at Interact 2005 in Rome, Italy. http://www.effin.org/egov-workshop_proceedings.html
8. Jena (2002). The jena semantic web toolkit, http://www.hpl.hp.com/semweb/iena-top.html, Hewlett-Packard Company.
9. Jena (2005). Jena - A Semantic Web Framework for Java, http://jena.sourceforge.net/
10. RDQL (2005). Jena RDQL, http://jena.sourceforge.net/RDOL/
11. Protégé (2005). Protégé, Stanford Medical Informatics. 2005.
12. Protégé-API (2006). The Protégé-OWL API - Programmer's Guide, http://protege.stanford.edu/plugins/owl/api/guide.html
13. Liberty Alliance Project. http://www.projectliberty.org/