Improvements of pan-European IDM Architecture to Enable Identity Delegation Based on X.509 Proxy Certificates and SAML

Sergio Sánchez García, Ana Gómez Oliva

Improvements of pan-European IDM Architecture to Enable Identity Delegation Based on X.509 Proxy Certificates and SAML

Sergio Sánchez García, Ana Gómez Oliva,

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

Abstract. To foster the secure use of telematic services provided by public institutions, most European countries – and others in the rest of the world – are promoting electronic identification systems among their citizens to enable fully reliable identification. However, in today's globalized environment, it is becoming more common for citizens and entities of a given country, with their own electronic credentials under the legal framework of their country, to seek access to the public services provided by other countries with different legal frameworks and credentials. At present, a number of projects in the European Union are attempting to solve the problem through the use of pan-European identity management systems that ensure interoperability between the public institutions of different Member States. However, the solutions adopted to date are inadequate, for they do not envision all possible cases of user interaction with institutions. Specifically, they fail to address a very important aspect provided in different national legal systems, namely delegation of identity, by which a citizen can authorize another to act on his or her behalf in accessing certain services provided by public institutions. This paper provides a thorough analysis of problems of delegation and proposes an architecture based on X.509 Proxy Certificates and SAML assertions to enable delegation in provision of services in the complex and heterogeneous environment presented by the public institutions of the European Union as a whole.

Keywords: Identity delegation, Proxy Certificates, SAML, X.509, eID, eIDM, electronic identity, electronic identity management systems.

1 Introduction

In the development of the information society, public authorities are playing an important role by promoting the implementation of new e-government services to enable citizens to perform administrative transactions quickly and easily. Given that dealings between citizens and the government are often of a strictly personal nature, there is now a growing demand for electronic or digital identity systems to unequivocally identify people on the Internet.

In recent years, initiatives are under way in all Member States of the European Union (EU), for the introduction of electronic identities (eID) in public services for the adoption of systems to manage them. In most EU countries, the electronic identity systems implemented are based on the use of electronic identification cards, also called eID cards, which are beginning to take the place of the identity cards now used in some countries. These cards include a chip that can both store citizens' identity information and interact with certain validation applications.

Although the introduction of a digital identity solves the principal problem of remote authentication of citizens, this solution is not sufficient on its own to achieve equivalence between administrative acts executed with traditional methods with those that can be undertaken by electronic methods, as there are other problems related to the different legal frameworks and different ways identity is used in each country. Of these problems, the most significant and most relevant one, owing both to its complexity and the fact that it is in demand from the public, is identity delegation. In fact present law in many Member States of the EU allows for delegation to another party in dealings with public institutions: for example, a citizen can delegate to a specialized service provider all interactions with the public institutions necessary in order to pay taxes.

However, the present problem of identity delegation in the public administration has hardly been addressed in scientific literature, perhaps owing to the more immediate need to deploy identity management systems in each country. Once this first phase of deployment has been completed, it is time to consider solutions that enable solving this problem not only at a national level, but a solution that is scalable for use in the complex and heterogeneous environment presented by the public institutions of the European Union as a whole. In Europe, circumstance occurs that although a citizen's electronic identity allows for operations within the system of one's own country, this is not the case when that system becomes that made up of all the countries of the European Union. Even though a German citizen traveling in Belgium can present his or her German identity card to prove their identity in dealings with the Belgian authorities, they cannot do the same thing with electronic identity, as the electronic identity and identity management systems in the two countries are not compatible.

Hence one of the central problems in the use of a digital identity is interoperability between identity systems at a pan-European level. Generically, owing to the diversity of identity management systems, when the user of a given system – whether a citizen, an enterprise or the government itself – seeks to communicate with governments outside the scope of his or her own local identity management system, management systems must be linked to each other and understand each other so that the identity of the user of one system can be understood and accepted by the other system.

This paper offers solutions to the problem of identity delegation, thus allowing citizens and entities to delegate to another person or entity certain interactions with public institutions. First, it provides a complete solution to the problem of identity delegation at national level, then, being based on the present state of

affairs in identity management systems at a pan-European level, where agreement in principle exists, proposing a model for interoperability between identity systems at a pan-European level that includes delegation. This will show the scalability and applicability of the model presented for communications with identity delegation among citizens and institutions from different EU countries. The paper also discusses the pilot project in progress for implementing the solution.

2 Digital Identity and Delegation of Digital Identity

The concept of **digital identity** or network identity, as it is called by the *Liberty Alliance* [1] has emerged from users' interaction with services offered on the Internet. When users interact with these services, they often personalize them according to their own preferences or needs: apart from establishing data access control such as user and password, they will define other parameters such as, for example, the information they wish to see displayed, the arrangement of items on the page offering the service or a method for notifying changes in the service. Users normally establish an account and personalize it for each of the service providers to which they accede. Thus, a given user will have multiple accounts with multiple parameters. According to the Liberty Alliance, the Network Identity of a user is the total sum of attribute sets of all a user's accounts.

Specifically, the draft *Liberty ID-FF Architecture Overview* [2] defines network identity as *the global set of attributes composed from a user's account(s).* For any given identity, there are usually several digital identities that may be unique or not. A digital identity is, by definition, a subset of identity and can be considered the manifestation of identity on the Internet.

The concept of **identity delegation** is defined by the Modinis IDM Study Team [3] as *the process in which an identified entity issues a mandate to another identified entity.* On the basis of this definition, we can see that the act of delegating is a cession by a person or entity of part of its rights to another in order to enable the latter to act on behalf of the former before a third party. In terms of citizens and public institutions, delegation basically involves one citizen granting another citizen authorization or a mandate that the latter can use, in the name of the former, to access services provided by institutions.

Academic literature offers several examples of systems of delegation conceived for different purposes and using different technologies. Notable among these technologies for their affinity to our purpose in this paper, are those presented in Komura et al. [4], Alrodhan et al. [5], Gomi et al. [6] and Welch et al. [7].

According to Peeters et al. [8] at least three parties are involved in the process of delegation: the delegator, the delegatee and the service provider. The delegator is a person or entity that shares, by means of what is usually called a delegation assertion, one or more of its privileges in accessing a service with another person or entity. The delegatee is the person who receives the privileges of the delegator, that is, the delegation assertion, and the service provider is the party which, as its own name indicates, provides certain services on demand to the delegatee after

the delegation assertion has been presented. In addition to these generic entities, and depending on the delegation process used, other entities may emerge, such as the identity provider or delegation authorities.

Taking this set of basic entities as a point of departure, Alrodhan et al. [5] presents a classification of delegation in two elementary models: the model of direct delegation and the model of indirect delegation. Direct delegation is when the delegator delegates all or a subset of his or her privileges to the delegatee, who makes use of them to access a service. The same process applies in indirect delegation, but through a series of intermediate delegatees.

We would highlight a series of aspects of delegation that were mentioned in Alrodhan et al. [5]. The first is that delegation does not mean authorization. That is, even if a service provider accepts the delegation, it need not accept the privileges requested by the delegatee. It is always at the discretion of the service provider whether or not to accept the request made by the delegatee. Secondly, the delegation assertion must always prove consent on the part of the delegator, as the latter may impose certain conditions on the act of delegation such as a period of validity or permission to engage in indirect delegation. Finally, any solution must always seek to preserve the privacy of the delegator.

3 Proxy Certificates, SAML and their Integration

As shown in the preceding section, a number of options for handling identity information are available (SAML, I-Card, etc.), each with its own benefits and drawbacks. However, the range of alternatives narrows if we wish to enable dynamic identity delegation and attribute-based restrictions. The authors have opted for the following features:

1. Use of Proxy Certificates, owing mainly to their ease of integration in present identity processes in European countries – most use public key certificates for authenticating users – and their possibilities for dynamic generation and
2. Use of SAML assertions with attribute statements for the transport of user attributes because this is the dominant trend in standardization and use.

We shall now discuss these technologies and how they can be integrate.

3.1 X.509 Proxy Certificates

X.509 Proxy Certificates [9] emerged as a result of certain needs that were not adequately met by X.509 public key certificates. The most obvious example is perhaps dynamic delegation, that is, the cession of a set of privileges by one entity to another for a very specific period of time. It is true that this type of delegation can be provided by other elements in the X.509 world, such as attribute certificates [10], but their use is not convenient owing mainly to the high degree of processing and the amount of time needed to generate them.

Identity certificates or public key X.509 certificates and Proxy Certificates have the same format, as they both link a public key to a name or Subject Name,

which allows Proxy Certificates to be used easily by libraries and protocols with no need for new implementations. However, unlike public key certificates, the entity that generates the Proxy Certificate is not a Certification Authority (CA) but rather an entity identified with a public key certificate or another Proxy Certificate, which facilitates enormously the process of certificate generation and makes the process of interacting with CAs superfluous.

All Proxy Certificates must contain a critical extension called PCI (Proxy Certificate Information) which not only identifies the certificate as a Proxy Certificate but also enables the certificate generator to express its desires with respect to the delegation of rights and to limit the number of Proxy Certificates that can be generated on the basis of the same. For the former, the PCI extension has a framework for the transport of delegation policies expressed in any policy language, with the sole restriction that the parties must be able to interpret the language and, hence, the policy defined.

The process to generate X.509 Proxy Certificate for delegation involves the following steps:

1. The delegatee generates a pair of keys, a public and a private one.
2. The public key is used by the delegatee to form a Proxy Certificate request to be sent to the delegator through an authenticated channel with an integrity guarantee.
3. The delegator checks that the request is correct and, if all is in order, the Proxy Certificate is generated. The certificate must be signed either with the private key of the generator or the private key of another Proxy Certificate.
4. The delegator sends the Proxy Certificate generated to the delegatee through an authenticated channel with an integrity guarantee.

It is evident that the process of generating Proxy Certificates is quicker and easier than that of X.509 public key certificates. The main advantage is that the process does not require the intervention of a CA.

3.2 SAML

This section provides a brief introduction to the SAML 2.0 [11], which is an XML-based language used to exchange authentication and authorization information between different entities in a network. SAML allows an entity to make assertions of security information on a subject through use of statements. Hence, an assertion linked to a subject may contain three different types of statements:

- *Authentication statements*: These indicate whether a user has been authenticated or not. If authentication has been completed successfully, they must, at least, indicate the method of authentication used and the specific time the authentication took place.
- *Authorization decision statements*: This specifies what the subject is eligible to do. It contains recommendations on access control, such as when a subject can or cannot access a resource.

– *Attribute statements*: These contain a specific set of subject-related attributes. For example, name, age and present employment.

The exchange of requests and responses of SAML assertions is performed with different communication protocols by means of binding. The most common method is to transport SAML messages over HTML, although SOAP is also commonly used.

3.3 Integration of SAML Attribute Statements and Proxy Certificates

One of the most important features of the architecture presented herein for identity delegation in public institutions is the integration of SAML attribute statements and X.509 Proxy Certificates. The idea emerged from study of the GridShib project [12]. The objective of the project is to enable interoperability between the Globus Toolkit® by Globus Alliance [13] and Shibboleth® by Internet2 [14] to attain secure exchange of attributes between Grid virtual organizations and institutions of higher education.

The GridShib project proposes an approach called X.509 binding for SAML [15]. This is a way of embedding SAML assertions in X.509 certificates, whether they are public key certificates or Proxy Certificates. It uses a non-critical extension of the X.509 v3 certificate, to which a single Object Identifier (OID) is assigned, that may be defined in ASN.1 as a *SEQUENCE of <saml:Assertion>*. In broad outline, every certificate can contain a non-critical extension that in turn contains a SAML assertion or a reference to it. If it has not been generated by the same entity that signed the certificate, the assertion must have been signed. If the entities match, the assertion signature is unnecessary, as the certificate signature covers the extension and, hence, the assertion. Linking the SAML assertions by means of a non-critical extension allows third parties to override the extension and therefore, enable normal use of the certificate in any environment.

This method of integrating SAML assertions in X.509 certificates, specifically in Proxy Certificates, constitutes one of the foundations for solving the problem of delegation as conceived for the pan-European identity management infrastructure proposed by the authors in the section that follows.

Specifically, the use of Proxy Certificates generated dynamically, exploiting the capacities of extensions and integration with SAML, offers the advantage of easy implementation of services with attribute-based delegation of identity and authorization, providing a flexibility of use that had barely been considered in previous architectures. Such flexibility has become a necessity owing to the frequent role representatives or agents play in traditional methods.

4 Proposed Delegation Model

Below we present the architecture conceived for delegation and its mode of operation. The proposal begins from the starting point explained in Welch et al. [7],

which presents a system for dynamic identity delegation by using X.509 Proxy Certificates in Grid environments, while adapting them to the use of Identity Providers and Service Providers in an electronic Identity Management System and integrating in X.509 certificates the part related to use of SAML attribute assertions and their transport.

For the presentation of participating entities and of the model of communication and performance, we shall start from a hypothetical case of use by a person, a German citizen for example, who seeks to obtain a service from an official institution but, for a number of reasons, is forced to delegate to a management company, who will perform all administrative steps on his or her behalf.

At first, the participating entities would be as follows:

- Delegator: The person or entity that cedes part of his or her privileges to another. In our example, it is a citizen who seeks to receive a service. In our example, the German citizen.
- Delegatee: The person or entity that receives the privileges from the delegator. In our example, the management company.
- Service Provider: The entity responsible for providing a certain service, either to the delegatee or the delegator. If the service provider supports providing services to delegatees, it must be capable of verifying that the delegation process has been performed correctly.
- Identity Provider: The entity responsible for authenticating users and generate authentication or attribute assertions. In our example, it would be the entity responsible for authenticating users in German public institutions.

The model of communication and interaction in providing a service with delegation is illustrated step-by-step in the figures below. The information flow sequence is as follows:

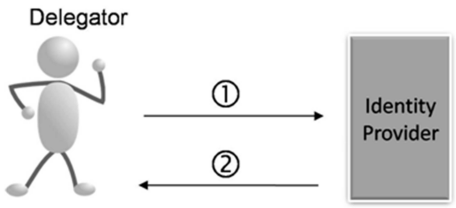

Fig. 1. Model of service provision with delegation: authentication

The steps shown in 1 and 2 depict the interaction of a citizen delegator with the Identity Provider and the initiation of communication with the delegatee. Figure 3 shows the final model of service provision with delegation of identity and revocation queries

1. The delegator presents his or her credentials to the Identity Provider with intention of being authenticated. Said credentials may be, for example, an

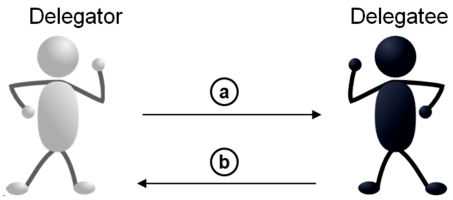

Fig. 2. Model of service provision with delegation: delegation of identity

X.509 public key certificate such as one presently used in some European Union countries. The delegator also requests a SAML assertion with an attribute statement that includes attributes needed for provision of a service through a delegatee.

2. The Identity Provider, after verifying the credentials of the delegator and that everything is in order, provides a signed SAML assertion with the set of attributes requested. It is the delegator's task to check that the attributes and the Identity Provider's signature are correct.
   (a) The delegator asks the delegatee to access the service in his or her name.
   (b) The delegatee, with the intention of obtaining a token to authorize said person to act as a delegatee vis-a-vis the service provider, generates a pair of keys – a public key and a private one – and sends the delegator the public key, while keeping the private key properly protected.

The Delegator shall build a Proxy Certificate for the key received, thus generating the delegation token. The Proxy Certificate will include, through a non-critical extension and in a manner that is similar to that proposed in [15], the SAML assertion with the attribute statement received from the Identity Provider and signed by the latter. Thus, the Proxy Certificate will also include, through a non-critical extension, identification of the service or services for which delegation is granted, so that the service provider can determine not only if the delegator has delegated access to services but also the services to which access has been delegated. To identify services, URIs (Uniform Resource Identifiers) [16] are used to achieve unequivocal identification. The use of URIs also provides another advantage, given their hierarchical structure: the delegator can specify if the delegation applies to only one service or to a set of services with a single provider .

3. The delegator sends the delegatee the Proxy Certificate generated.
4. Once the delegatee is in possession of the Proxy Certificate, it also has the token that will allow it to request the service from the Service Provider.

The Service Provider checks the validity of the Proxy Certificate and verifies that the validation path is correct. The Proxy Certificate is linked to the delegator by the signature, so the Service Provider will know in whose name the delegatee is acceding to the service. On this basis, and that of the SAML assertion with the attribute statement and the URI of the allowed services included in the

pertinent extensions, the Service Provider can make decisions of authentication and authorization that will enable it to determine whether to provide the service.

5. Assuming that everything is in order, the Service Provider delivers to the delegatee information on service requested.
6. The delegatee then delivers to the delegator the results of the service.

As we can see, step 2 (Fig. 1) consists of a signature verification that involves interaction of the delegator with the PKI to verify whether the certificate of the Identity Provider has been revoked. In addition, after step 4, (Fig. 3) the Proxy Certificate is verified. As defined in the RFC 3820 [9], a process must be undertaken in such a way that to complete verification of this type of certificate we must check, first of all, that the certificate of the entity generating it, in our example the public key certificate of the delegator, is valid under the verification procedures of PKI as defined in the RFC 3280 [17]. Moreover, for a Proxy Certificate to be considered valid, the following must be carried out:

1. For all x in {1, ..., n-1}, the subject of certificate x is the issuer of proxy certificate x+1 and the subject distinguished name of certificate x+1 is a legal subject distinguished name to have been issued by certificate x.
2. Certificate 1 is valid proxy certificate issued by the end entity certificate whose information is given as input to the proxy certificate path validation process.
3. Certificate n is the proxy certificate to be validated.
4. For all x in {1, ..., n}, the certificate was valid at the time in question.
5. For all certificates in the path with a length constraint field, the number of certificates in the path following that certificate does not exceed the length specified in that field.

Nevertheless, and bearing in mind the above, there is still a problem with using Proxy Certificates: no procedures have yet been defined for revoking this type of certificates. There are applications in which, owing to the specific and restricted use of these certificates, they are unnecessary. However, in our case, owing to the numerous possible types of use, this type of mechanism is indispensable. Thus, the architecture includes a new entity, a Proxy Certificate Revocation Authority. Like Revocation Authorities in the present PKI, it maintains a listing of certificates, specifically Proxy Certificates, that have been revoked.

In ADMISSION project we propose the use of Proxy Certificate Revocation Authorities for each one of the national eIDMs to manage the status of the Proxy Certificates that have been issued by the entities in it. Each of the Proxy Certificate Revocation Authorities has a revocation list in which every issuer of Proxy Certificates is associated to a list of certificate identifiers issued by it that have been revoked. It would also enable querying and updating of the list. Owing to its functionality, it has been decided that the Proxy Certificate Revocation Authority will be included as a Trusted Third Party (TTP) in the PKI infrastructure being used. tThe process of querying the revocation status of the Proxy Certificate by the Service Provider is depicted as steps 4a and 4b, yielding the final proposal for a communication model as shown in Fig. 3.

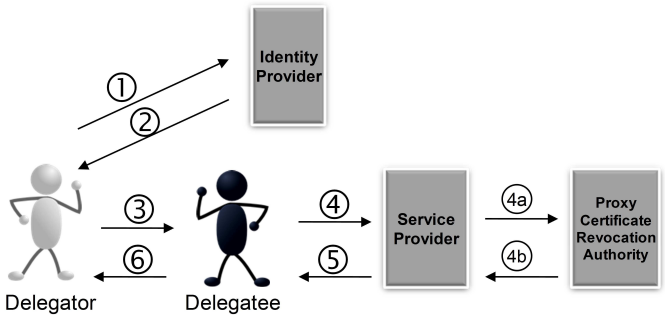

Fig. 3. Model of service provision with delegation of identity and revocation queries

At present, the authors herein are working on the implementation of a pilot project based on the proposed infrastructure for managing identity and providing services both with and without delegation of identity in the a City Council in the region of Madrid, with a view to proving the viability of the solution and its possibilities. The pilot project is being implemented in a real scenario at a small scale, involving a circle of trust with several Service Providers (SPs) and an Identity Provider. We have selected a number of telematic services that the city council will soon offer on the Internet: applications for tax rebates and exemptions, applications for authorizations (such as permits to set up a newsagent, pavement cafes, bars in the public highway, to allow use of cranes, etc) and applications for operating licenses. Each of these services is offered through a different Service Provider that can process demands from citizens and delegatees, but all within the same circle of trust. To enable access to these services, identification of citizens is to be performed with an X.509 digital certificate embedded in their National Identity Card (eID Card) or another digital certificate issued by a Certification Authority accepted for transactions in national public institutions. Verification of citizens' identity is performed by the Identity Provider of that circle of trust.

We are now capturing the attribute requirements necessary for citizens to access services and defining SAML assertions with attribute statements on this basis. Simultaneously, we are working on the implementation of identity delegation in the same testing environment with a view to achieving a complete identity management solution with support for delegation.

5 Scalability and Applicability of the Proposed Solution at a pan-European Level

Nowadays, Europeans are living in an environment that is not only increasingly digitalized, but which is increasingly globalized. A citizen of France 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 French 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 French national?

5.1 Problems of Interoperability

Answers to the questions posed above are no simple matter. 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 established in each European Union country. 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.

One of the first studies or projects related to interoperability of identity management systems was the Modinis eIDM Study [18], which studied the use of electronic identity management systems in the European Union and analyzed the most significant consequences of using these eIDM systems.

Another interesting system is the TLS-Federation [19]. 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 GUIDE project (*Creating a European Identity Management Architecture for eGovernment*) [20] 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 that requires membership in circles of trust based on operational agreements, thus yielding a federation of service providers and identity providers. 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*) [21]. 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.

As part of the research project ADMISSION, we have analyzed the problem of identity management at all levels of public institutions, from the local level to

Europe as a whole. After a detailed study of identity management at the local, regional, provincial and national levels, we reached the conclusion that problems of interoperability that exist between the member countries of the European Union in managing citizens' identities are also found in the interaction between different levels of institutions, even within a single country. We propose herein a model of interoperability that may be applied not only at a pan-European level, but also at lower levels, i.e., nationally, regionally or locally. It would guarantee interoperability in identity management at all levels. The model builds on the beneficial features identified in the identity management systems discussed herein and solves the problems detected in them.

Federation, achieved by establishing circles of trust at each level and between levels, as shown in Fig. 4, is the basis of the proposed system.

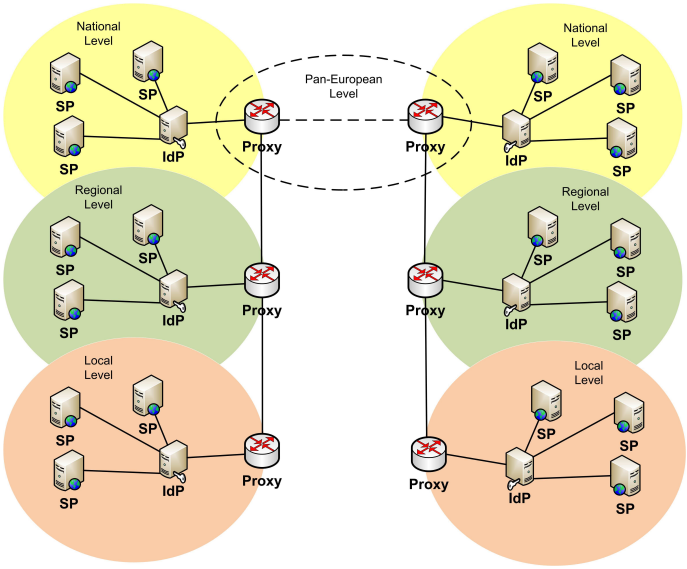

Fig. 4. Infrastructure proposed in ADMISSION project

The chart shows how each level of government – local, regional and national – has a circle of trust that links together one or more Identity Providers (IdP) and Service Providers (SP) at that level. To attain reliable authentication of individuals, it will use token mapping: that is, it will allow for maintaining present systems and map currently used authentication elements to common elements in order to guarantee interoperability of services. This is a fundamental principle, as the deployment of services offered by public institutions has grown in an uncoordinated fashion for quite some time, and they often provide services that are highly valued by citizens. Thus, the system uses the concept of proxy as an interface between identity management systems to ensure interoperability both

at the same level – for instance, local interoperability between two or more city councils – and between levels; for example, between a city council and a hierarchically higher level: a provincial, regional or national institution. Exchange of authentication tokens will use X.509 certificates, the use of which is familiar to all official institutions.

5.2 Problems of Electronic Signatures

In addition to the problems of interoperability between different identity management systems discussed above, there are other interoperability problems that have a greater impact for because they are directly related to our delegation solution, namely electronic signatures. The ultimate interoperability situation for e-signatures and any other use of eIDs can be stated as:

- An eID holder shall be able to use the eID to sign a piece of information towards any counterpart, even internationally. The eID holder independently selects the eID to use.
- The receiver (relying party) of a signed document shall be able to accept signatures from all counterparts, regardless of the eID used by the counterpart.
- A third party, receiving a document signed by other parties, shall be able to verify the signatures no matter the eIDs used by the other parties.

The relaying party role is clearly the one facing the complexity. The eID holder has one trusted party to rely on: the Certification Authority (CA). The relaying party must check all signatures, handling the relevant signature formats (includig all necessary modes) for multiple signatures, all necessary hash and crypto algorithms and the eIDs of all signers. Although the technical validation of signatures has its challenges with respect to scaling, the real problem to the relaying party is the assessment of the risk implied by accepting the signature, determined by the legal situation, the quality of the cryptography used, the liability situation, and the trustworthiness of the CA. With the objective of solving these problems, the European project PEPPOL [22] is developing guidelines, specifications and pilot solutions to overcome the lack of interoperability between national schemes for electronically signing tender documents.

5.3 Explanation of Scalability

As is clear from the foregoing, the possible use of our delegation solution in a pan-European scenario is not a simple matter, as things stand today. Nevertheless, we can say that the solution proposed to interoperability problems in identity management is following the same trends as other European initiatives undertaken to date. This solution fits perfectly into our interoperability proposal and, therefore, allows for setting up a model of identity delegation that can be used at a pan-European level. As we have mentioned, the interoperability model is based on the establishment of circles of trust at different levels of public administrations in each country and between all countries. As X.509 certificates

present in the citizen identity cards are usually applicable at all levels of administration, it would be no problem to generate delegation at one level – whether local, regional or national – or between levels in one country. The main problem may arise in relation to revoking Proxy Certificates of the delegation, but as proposed above, inclusion of the Proxy Certificate Revocation Authority as a Trusted Third Party in the national PKI infrastructure provides a solution.

A different problem arises if one wishes to establish our model at a pan-European level: that is, we wish to set up an identity delegation system that would work between citizens and institutions of different countries. The main drawback lies in the above-mentioned problem of interoperability of electronic signatures, given that our delegation solution is based on the generation of Proxy Certificates that, as we have seen are directly signed by the delegator. A delegatee or a Service Provider in a country other than that of the delegator would find it difficult to verify the Proxy Certificate used in the delegation. Nevertheless, it would seem clear that the work and interest shown by the European Union in initiatives and action plans like the *i2010 eGovernment Action Plan* [23] in achieving total interoperability and a more global environment in European public administration obliges us to assume that total interoperability will be in place in the medium term for Europe-wide electronic signatures, thus making our delegation fully viable. Figure 5 shows a diagram of the pan-European global interoperability solution to support identity delegation, assuming that interoperability of electronic signatures has been attained.

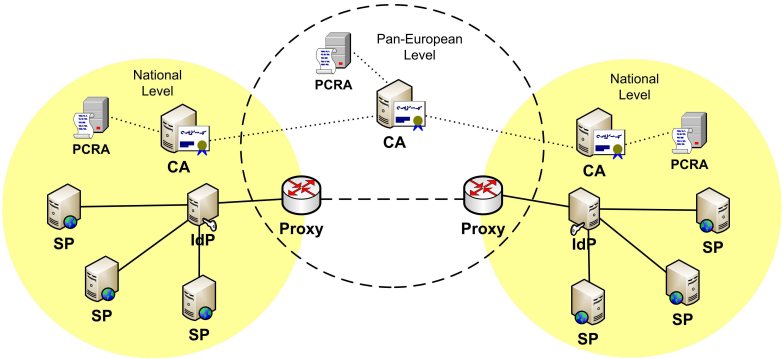

Fig. 5. Global infrastructure for interoperability and identity delegation

As we can see, two national environments and a pan-European environment are depicted, each with their IdP and SP and linked together through proxies that enable pan-European interoperability in identity management. Further, the PKI is depicted in each of the national environments through the Certification Authority (CA), and their communication with the Proxy Certificate Revocation Authority (PCRA), as required in our delegation solution given that no pan-European PKI exists, we have assigned the national PKIs the same level

and assumed a relation of trust between them. With a view to enabling the architecture to accommodate countries that lack their own PKI, the diagram depicts, also at the same level, a CA with its own PCRA at the pan-European level, thereby facilitating the addition of new countries.

6 Conclusions

The solutions to identity management problems in international environments will undoubtedly facilitate citizens' access to services in an ever more globalized world, while opening the door to ever more sophisticated and secure telematic services. With this in mind, the EU has set in motion a number of initiatives to develop and implement a pan-European identity management infrastructure. It is committed to solutions that will not force modifications in the national digital identification systems as developed by each country in accordance with its own needs and laws. But such solutions must be sufficiently reliable and robust to win acceptance in every country of Europe.

Although the range of solutions available is broad, important issues remain to be solved in most of them, such as the lack of integration with the private sector, the absence of single data sources to ensure the uniqueness and coherence of information on entities, the lack of solutions for identity delegation and problems related to the use of certain standards.

Therefore, the project undertaken by the authors' research group is oriented towards seeking solutions to these problems at two distinct levels. First, the solutions should have an echo in Europe; thus, we are in regular contact with the leading groups working in this field. Second, we are seeking to extrapolate our solutions to our national public institutions, where problems of interoperability between identity management systems at different institutional levels are similar to those in Europe. Consequently, we aim to make contributions that can support progress towards total interoperability in identity management both at national and pan-European levels to enable provision of services in a way that is simple and fully transparent to users. To address one of the main inadequacies of identity management systems proposed to date, our model integrates in the Global infrastructure for interoperability a solution for dynamic identity delegation based on X.509 Proxy Certificates and SAML assertions with attribute statements, thus yielding a pan-European identity management infrastructure with support for identity delegation.

References

1. Liberty Alliance Project, `http://www.projectliberty.org`
2. Wason, T. Liberty ID-FF Architecture Overview. Version: 1.2-errata-v1.0. Liberty Alliance Project (2005);, `http://www.projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf`

3. The Modinis IDM Study Team; Modinis Study on Identity Management in eGovernment: Common Terminological Framework for Interoperable Electronic Identity Management. Version 2.01. eGovernment Unit, DG Information Society and Media, European Commission, November 23, 2005.
4. Komura, T.; Nagai, Y.; Hashimoto, S.; Aoyagi, M. and Takahashi, K. Proposal of Delegation Using Electronic Certificates on Single Sign-On System with SAML-Protocol. In SAINT '09. Ninth Annual International Symposium on Applications and the Internet. 20-24 July, 2009.
5. Alrodhan, W. and Mitchell, C. J. A Delegation Framework for Liberty, In Proceedings of the 3rd Conference on Advances in Computer Security and Forensics (ACSF'08), pages 67–73, 2008.
6. Gomi, H.; Hatakeyama M.; Hosono S. and Fujita S. A delegation framework for federated identity management, In Proceedings of the 2005 workshop on Digital identity management, November 11, 2005, Fairfax, VA, USA.
7. Welch, V.; Foster, I.; Kesselman, C.; Mulmo, O.; Pearlman, L.; Tuecke, S.; Gawor, J.; Meder, S. and Siebenlist, F.; X.509 Proxy Certificates for Dynamic Delegation. 3rd Annual PKI R&D Workshop, 2004
8. Peeters, R.; Simoens, K.; De Cock, D. and Preneel B. Cross-Context Delegation through Identity Federation, In Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Lecture Notes in Informatics (LNI) P-137, A. Brömme, C. Busch, and D. Hühnlein (eds.), Bonner Köllen Verlag, pp. 79-92, 2008.
9. Tuecke, S.; Welch, V.; Engert, D.; Pearlman, L. and Thompson, M. Internet X.509 Public Key Infrastructure Proxy Certificate Profile. RFC3820, IETF, June 2004
10. Farrell, S. and Housley,R. An Internet Attribute Certificate Profile for Authorization, RFC 3281, IETF, April 2002
11. Ragouzis, N.; Hughes, J.; Philpott, R.; Maler, E.; Madsen, P. and Scavo, T. Security Assertion Markup Language (SAML) V2.0 Technical Overview - Committee Draft 02, March 25, 2008; http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf
12. GridShib. http://gridshib.globus.org/
13. Globus Toolkit®. http://www.globus.org/toolkit/
14. Shibboleth®. http://shibboleth.internet2.edu/
15. https://spaces.internet2.edu/display/GS/X509BindingSAML
16. Berners-Lee, T., Fielding, R. and Masinter, R.; Uniform Resource Identifier (URI): Generic Syntax. RFC 3986, IETF, January 2005.
17. Housley, R.; Polk, W.; Ford, W. and Solo, D. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, IETF, April 2002.
18. ModinisIDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome
19. Bruegger, B. P.; Hühnlein, D. and 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
20. GUIDE, Creating a European Identity Management Architecture for eGovernment, http://istrg.som.surrey.ac.uk/projects/guide/overview.html
21. STORK, Secure idenTity acrOss boRders linked, http://www.eid-stork.eu/
22. PEPPOL, Pan-European Public Procurement Online. http://www.peppol.eu/
23. Commission of the European Communities; i2010 eGovernment Action Plan: Accelerating Government in Europe for the Benefit of All. Brussels, April 2006. http://ec.europa.eu/idabc/servlets/Doc?id=25286