2009

A Cooperation Infrastructure For Communication Between Public Bodies; The Friuli Venezia Giulia Case

Francesco Sasso
Insiel S.p.A, Francesco.sasso@insiel.it

Margherita Forcolin
Insiel S.p.A, margherita.forcolin@insiel.it

Gilda De Marco
Insiel S.p.A, gilda.demarco@insiel.it

INTEROPERABILITY OF PUBLIC IS INFRASTRUCTURES

A COOPERATION INFRASTRUCTURE FOR COMMUNICATION BETWEEN PUBLIC BODIES; THE FRIULI VENEZIA GIULIA CASE

Sasso, Francesco, Insiel S.p.A., via s. Francesco 43, Trieste, 34133, Italy, Francesco.sasso@insiel.it
Forcolin, Margherita, Insiel S.p.A., via s. Francesco 43, Trieste, 34133, Italy, margherita.forcolin@insiel.it:
De Marco, Gilda, Insiel S.p.A., via s. Francesco 43, Trieste, 34133, Italy, gilda.demarco@insiel.it:

Abstract

Long ago, Italian Public Administrations started a process to increase the efficiency of their administrative procedures, adopting ICT technologies and tools in place of paperwork, but the approach was not structured nor synchronized. The result now is that Public Authorities' legacy systems are based upon heterogeneous and vendor specific solutions. To increase their efficiency is one of the most challenging issues that Public Administrations are facing in the latest years in order to ensure a faster communication among public bodies, avoid data redundancy and improve the service provided to citizens. The key element is to increase the cooperation among public bodies allowing a seamless communication which will not modify the already existing systems. The Friuli Venezia Giulia Region interoperability framework, presented in this paper, provides a layer which ensure the communication between Administrations increasing the efficiency of administrative procedures, through the adoption of secure electronic communication, and lead to the delivery of a better public service in terms of content and response time.

Keywords: *Interoperability, Egovernment, Data Exchange, Efficiency, Framework*

1 THE CONTEXT: INSIEL AND THE FRIULI VENEZIA GIULIA REGION'S EXPERIENCE

The modalities of interaction between public administrations assume a strategic role within the eGovernment priorities. Efficiency inside Public Administration is essential to guarantee a qualitative public service to citizens, which particularly means responding quickly and precisely to their needs. The objective is enabling the citizen to have a unique access point to administrative services (unique virtual counter), thus eliminating the need to move to different public offices. This goal can be reached by adopting solutions for interoperability between heterogeneous systems, so that a unique information system can integrate services delivered by different administrations.

In Italy, the national guidelines in this sector are contained in a document called "National Network: applicative architecture", which refers to:

- The Public Connectivity System [SPC1], infrastructure for the exchange of data and services between all central and local Public Administrations and Institutions;
- The Public System for Application Cooperation [SPCOOP2], integrated in the SPC, which concerns those interoperable solutions that are "neutral" with respect to the technological choices and service policies adopted by each Institution.

The Autonomous Region "Friuli Venezia Giulia" commissioned Insiel, the ICT company owned by the Region, the design, development and management of a regional interoperability framework which

could virtually connect all local public authorities, health institutions and hospitals on the regional territory. The regional interoperability framework is based on two main systems:

- the Domain Gateways;
- the Identification/Authorization system,

through which the communication and data exchange between different public organizations is guaranteed, as well as the data access management.

The regional interoperability framework realized by Insiel enabled Public Administration to increase the efficiency of its administrative procedures, adopting electronic communication in place of paperwork, and lead to the delivery of a better public service in terms of content and response time.

Another goal reached by the regional interoperability framework is the possibility the citizen has to choose which modality he/she prefers, to access public services, whether the traditional one (public office counters) or the internet channel, which avoids having to personally go to the offices concerned. The interoperability project extended the range of public services made available to the citizen by conveying data coming from different public bodies to the regional Portal, that the citizen can access, using a smart card named Regional Services Card, in absolute security.

On the basis of Insiel's experience in the Friuli Venezia Giulia region, the following considerations may be made on the interoperability framework that was adopted:

- the structure based on domain gateways and on a federated identification/authorization system enables to identify different operators in a non redundant and secure way authorizing them to access resources and exchange data in a secure way;
- it did not require to change the existing legacy systems of participant Administrations and this brought to low deployment costs and times;
- efficiency in Public Administration has increased, both in internal procedures and in its relationship with citizens.

2 THE PRINCIPLES OF APPLICATION COOPERATION

Application cooperation enables heterogeneous systems (different operating system, implementation language, management system or access to resources) to exchange services on the basis of standardized messages and therefore easily understandable by each system.

As stated above, the Public Connectivity System (SPC) defines the connectivity infrastructure and the way in which cooperation should be carried out in order to respect each Institution's independence. Moreover SPC defines the cooperation model as follow:

- each Organization is considered a Domain
- the National Network is seen as a federation of domains;
- each Domain is identified with all the resources (procedures, data and services) and service policies of the given organization;
- defines a cooperation architecture that enables the integration of the resources (procedures and data) from different domains, regardless of the legacy systems of the single domain;
- uses Internet standard protocols (mainly HTTP but also SMTP and FTP) as reference for data transmission between domains;
- Identify the standards to be used for service requests between Organizations that are XML (eXtensible Markup Language) to define a data format easy to be shared between heterogeneous systems, SOAP (Single Object Access Protocol) to convey the XML-coded information over the

network, through HTTP/HTTPS protocol and the eGovernment-Envelope to wrap and secure the communication.

3 THE DOMAIN GATEWAYS

The so called **Domain Gateways** are the key technological component of the application cooperation architecture compliant to the **SPC** (Public Connectivity System). They represent the unique and exclusive access point to the resources of a given organization and correspond to a set of (software) functionalities that can be activated within each domain, both to allow access to the organization's resources and to access other domains' resources, without significantly changing the existing environment.

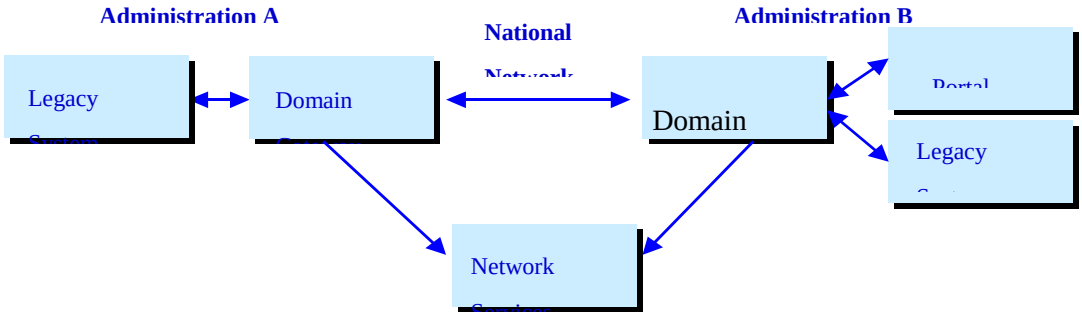

Figure 1 Reference model for the integration of Domain Gateways

The assumptions on which the Domain Gateways (figure 2) are based, are the following:

- each domain can be considered a client domain or a server domain, depending on the fact that they are requesting a service or responding to a service request;
- the Gateways are called Delegated Gateways when they request a service and Application Gateways when they provide a service (Figure 3).

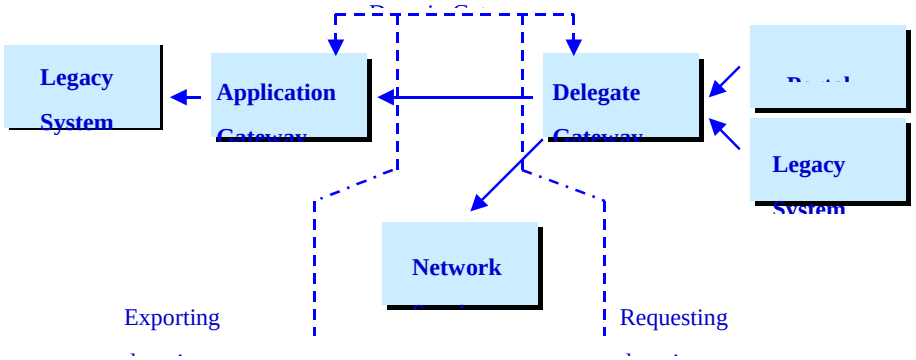

Figure 2 Domain Gateways Schema

The technical architecture of the **Domain Gateways**, although established within each domain, is characterized by the following aspects:

- a three-level architecture compliant with SPC specifications (client domain, Domain Gateway and server domain);
- screen the specific legacy system details (of a given administration), while exposing the administration's services on the SPC utilizing standard representations based on XML.
- they can be implemented through web service-based solutions;

- Administrations can cooperate over the network accessing a specific network service, the Domain Registry, where for each domain are listed the available services and their interaction model.

To ensure interoperability towards external institutions, a Domain Gateway is connect to the **Public System of Application Cooperation** (**SPCOOP**). Integration enables access to the services therein made available by local and central public authorities also enabling the latter to receive specific services from other organizations. The **ESB** enables the link between the Domain Gateway and the application components and all the specific functionalities that ensure the interaction between domains are invisible to applications.

4 IDENTITY & ACCESS MANAGEMENT

The proposed model is based on the federation of the domains involved in the project, which communicate with one another through the network. The aim is ensuring the transparency from the legacy level of the services offered by each domain, considering the specific modalities of interaction used within the domains themselves.

The domain interface conceptually represents the entrance point enabling access to the applicative resources offered by the domain. It can be further specialized in the **portal** and the **domain gateway**: the first dealing with the interaction between human users (i.e. citizens) and services, the second being the access point for software applications intending to access the services offered by the domains. Furthermore, the domain gateway represents the point of access towards other domains, with regards to the services defined within each domain and a domain interface will enable each domain to access the services made available by other domains.

It can be noticed that generally the two modalities of access to a service correspond to two different levels of interaction between the involved actors (users and other domain services). The first level enables communication between the user's browser and the service front-end, the second level connects the front-end to one or more back-ends. The first interaction is, as usually happens, between a browser (also called User Agent) and a web server. The second one takes place, in an application cooperation perspective, between the domain gateways of the different institutions which participate in the implementation of the service requested by the user. This paper aims at illustrating the modalities for identity certification and authorization verification in both phases, for all the subjects involved.

The system is based on the **SAML[3]** protocol. SAML servers are dedicated to assertion delivery. The SAML protocol operates with three standard types of assertions, the **Authentication Assertion** issued by the **Identity Provider (IDP),** where the server certifies that the user subject to assertion has logged in using the modality described in the assertion itself, the **Attribute Assertion** issued by an **Attribute Authority (AA**), in which the server certifies that the subject concerned by the assertion possesses certain attributes, and the **Authorization Assertion** issued by a **Policy Decision Point (PDP**) that decides on the authorization to be given to a principal requesting access to a specific resource. The model functions in a very simple way: the server responds to each type of request with the related assertion.

The **Profile Authority (PA**) is a system where the user can register, in a personal profile, all the attributes possessed and the related certifying bodies or **Attribute Authorities (AA).**

The case we will take into consideration concerns a generic user or principal, possessing an **Authentication Assertion** issued by an **IDP**, wanting to access a service of interest. First of all, the user will need to access the responsible SAML server (AA), that will deliver an Attribute Assertion with one or more attributes associated to the user. Then, the user, providing the received assertion, will request a specific service; another SAML server (PDP) will check that the user is authorized to access the service requested, either by delivering an Authorization Assertion or by specifically creating an individual authorization based on the user's identity.

4.1 Profile Authority (PA)

Which are the necessary attributes to access a given service? Once attributes are defined, to which **Attribute Authority** should the **Attribute Assertions** be requested to certify the user?

Two informative structures are available and provide the solution to both enquiries: the **User Profile** and the **Service Profile**.

The Application Domain manages the Service Profile which is published in the associated Services Registry. The Service Profile lists the necessary attributes to access the service, and, in addition, it can also indicate the Attribute Authority. The Service Profile enables a correct composition of the **Assertion Portfolio**. If an Assertion were missing, the Application Domain would proceed with the integration of the Portfolio.

It is the user who directly manages the User Profile, indicating Attributes and referring to the respective Attribute Authorities. To make it available for the federation, the User Profile could be inserted in a Registry or delivered as an Attribute assertion by the Attribute Authority of the user.

No privacy or security issues are raised by the two Profiles, with regards to the data managed.

4.2 The proxy/deputy

Some **Access Policies** may need a written proxy from a third party. The third party could be the owner of the information related to the request or there could be role proxies, etc. From a formal point of view, the Proxy is nothing else than an **Attribute Assertion** which links the requesting entity to the delegating subject for one or more services.

4.3 Identity Provider (IDP)

The Single Sign-On currently used throughout the Web implies a unique authentication by the user, to a website, through which he/she can access a second website and its resources without having to proceed with a second authentication. The integration of the Single Sign-On with the communication of the **Identity Assertion** enables the second site to consider the user directly authenticated, trusting the origin of the assertion. In fact, in this case, the first site acts as **Identity Provider**.

This scheme is also valid for cases of application cooperation in which the systems providing services do not possess front-end features through which users can be directly authenticated.

The same **Identity Assertion** can be used several times (in a given limited time period) and by different systems. The most important factor is the trusted relation between the producer of the **Identity Assertion** and the entity that uses it to enable access to its services. The confidentiality of the relation is guaranteed by classical mechanisms such as the digital signature and the consequent public credentials made available and guaranteed by a recognized **Identity Provider**.

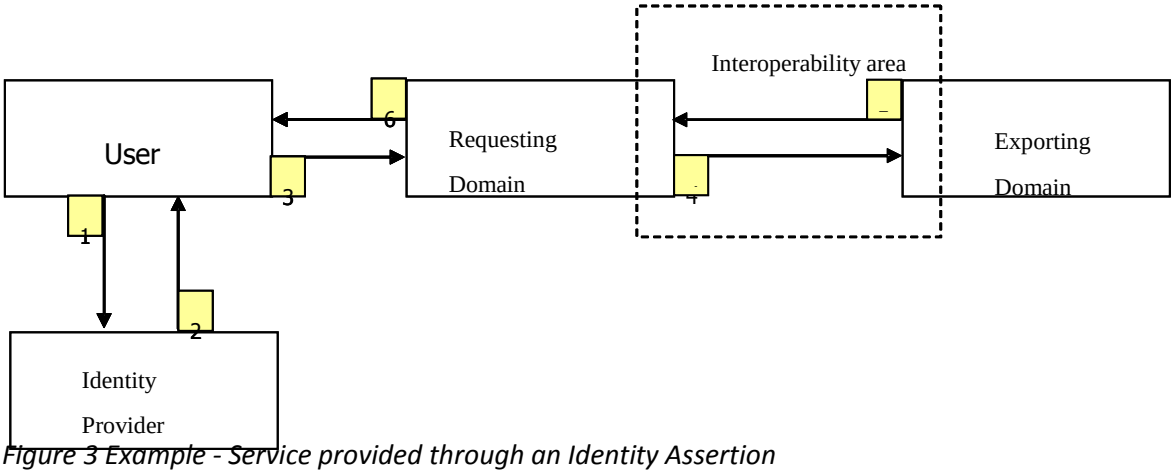

Figure 3 Example - Service provided through an Identity Assertion

1. The user authenticates on the Identity Provider
2. The user obtains an Identity Assertion from the Identity Provider
3. The Identity Assertion and the service request are sent to the Requesting Domain
4. The Requesting Domain links the Identity Assertion to the request and sends them to the Exporting Domain
5. The Exporting Domain recognizes the User and provides the service
6. The user receives the service or an exception

4.4 Attribute authority (AA)

A user may be characterized by numerous *attributes* that do not depend on the **Identity Provider**. These are, for example, the role a user plays in an organization or Domain, the title, determined by registration to a Register or an officially recognized status.

Attributes are the main elements which determine the **Access Policies**.

Attributes characterize an identity with reference to one or more application context. Each attribute associated to an identity has the validity assigned by the related **Attribute Authority.**

The same **Attribute Assertion** can be used several times (in a given limited time period) and by different systems.

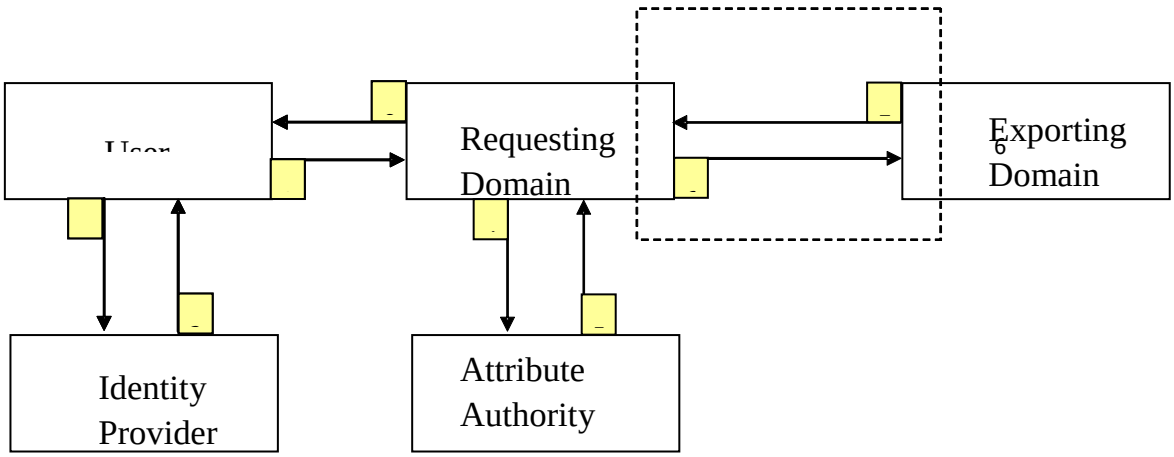

Figure 4 Example – Service provided through an Attribute Assertion

1. The user authenticates on the Identity Provider
2. The user obtains an Identity Assertion from the Identity Provider
3. The Identity Assertion and the service request are sent to the Requesting Domain
4. The Requesting Domain sends the Identity Assertion to the Attribute Authority, asking certification of the Attributes that are necessary for the service requested
5. The Attribute Authority issues an Attribute Assertion for the attributes requested
6. The Requesting Domain links the Identity Assertion and the Attribute Assertions to the service request and forwards them to the Application Domain
7. The Application Domain recognizes the user AND/OR the attribute and delivers the service
8. The user receives the service or an exception.

4.5 Policy Decision Point (PDP)

An Application Domain can deliver a service upon receipt of an Authorization Assertion issued by the Policy Decision Point for that Domain. The PDP checks the Identity and Attribute Assertions received together with the service request and, after interpretation of the Access Policy (defined for the specific service) which can depend on other data, issues an Authorization Assertion, which simply gives an indication of assent or denial.

Likewise other Assertions, the Authorization Assertion can also be used several times and by different systems, but this is not likely to happen very often because it would imply depending on a unique PDP and in an unchanged Application environment. Whereas in the other cases seen above we highlighted the existing trusted relation between the subjects involved, in this case it is more appropriate to speak of a solid and secure relation between the producer of the Authorization Assertion and the entity that interprets it in order to deliver the Services.

4.6 Applications

The architecture presented in this paper has been initially tried out within two projects co-funded by the Italian Ministry for Technological Innovation (MIT):

- [IESS] - Integration system providing health services
- [SIRVINTEROP] – Interoperability framework for the Veneto Region.

Later on the results have been used by CNIPA (National IT Centre for Public Authorities) to define the national SPCoop infrastructure specifications.

Numerous Public Administrations had implemented their own Domain Gateways within the ICAR project [ICAR] utilizing other technologies compliant with the specifications, and the communication among different institutions has been verified between the Friuli Venezia Giulia region and other entities or regional administrations (Tuscany, Basilicata, Puglia, Liguria among others).

4.7 Possible applications in B2G and B2B contexts

Although they were developed to enable collaboration between different public administrations, the regional interoperability framework and the federated authentication can actually be used for communication between private **companies and public administration (B2G)** or for communications carried out by **private companies with one another (B2B).**

The Friuli Venezia Giulia government provided access to the regional interoperability framework both to all public offices and Regional and SMEs.

SMEs must implement their own domain gateways (Delegated and Application) and subscribe to an identity provider (e.g. those managed by trade associations) that can certify the identities and/or professional roles of the different users. The company should obviously declare which services it will make available through the domain gateway and which roles can access the specific service.

SMEs can download the software components that enable them to implement the domain gateways from a regional Portal (the solution is based exclusively on open source components and available under eu-GPL license), from which they can also offer and receive software and services and develop new solutions that give them a competitive advantage.

In this way, they also contribute to the improvement and evolution of information systems and technology.

5 CONCLUSION AND LESSON LEARNED

From the overview of the process that brought to the effective development and dissemination of Application Cooperation throughout the regional Information System of the Friuli Venezia Giulia region, we can highlight and keep in mind two important aspects.

The first important element in Friuli Venezia Giulia's experience is the amount of time and resources spared: the deployment of the regional interoperability framework and the definition of services' access policies were carried out with a limited budget and in a very short time period, which are two characteristics of a modern and efficient public administration.

The second very important aspect is that neither internal procedures nor organizational structures had to be changed, in any of the public administrations involved. In fact, employees were able to continue carrying out their ordinary office work without changing any of their habits, during and after the implementation of the new interoperability system. This is quite an important achievement because, just as consistent expenditures and investments and long term efforts are feared by public officers and managers, organizational change is the greatest difficulty on the employees side, and can create a real barrier to the adoption of innovative IT tools and systems.

Both these obstacles were avoided by the analysts and developers who studied and carried out the project for Friuli Venezia Giulia's Application Cooperation Framework, making this infrastructure a model that can be easily and successfully re-used in other contexts.

References

http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/SistemaPubblicodiConnettivit%C3%A0 (SPC)/ (last accessed April 28th 2009

http://www.spcoop.it/ (last accessed April 28th 2009)

http://en.wikipedia.org/wiki/SAML (last accessed April 28th 2009)

http://www.regione.veneto.it/Servizi+alla+Persona/Sanita/Sistema+Informativo+Socio+Sanitario+e+Tecnologie+Informatiche/Progetto_IESS.htm (Last accessed 25 march 2009)

http://www.regioneveneto.net/progetto-sirv-interop (Last accessed 25 march 2009)

http://www.progettoicar.it/ViewCategory.aspx?catid=0803b58e331b419ab2967ce95899a386 (Last accessed 25 march 2009)