A Service-Oriented Integration Platform to Support a Joined-Up E-Government Approach: The Uruguayan Experience

Laura González[1], Raúl Ruggia[1], Jorge Abin[2], Guzmán Llambías[1,2], Raquel Sosa[1], Bruno Rienzi[1], Diamela Bello[2], and Fabricio Álvarez[1,2]

[1] Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Uruguay
{lauragon,ruggia,gllambi,raquels,brienzi,falvarez}@fing.edu.uy
[2] Agencia de Gobierno Electrónico y Sociedad de la Información, Uruguay
{jorge.abin,guzman.llambias,diamela.bello,
fabricio.alvarez}@agesic.gub.uy

Abstract. E-Government Platforms have become a key tool to support the development of e-government in many countries. They usually provide infrastructure and services that facilitate the interconnection between the information systems of public agencies, provide common services that generate economy of scale, and encourage the implementation of multi-agency services. In particular, the Uruguayan E-Government Platform has the general goal of enabling and promoting the development of e-government services in Uruguay. The platform, which follows a joined-up approach, consists of an Interoperability Platform and a set of Crosscutting Services. It implements a service-oriented architecture, leveraging the Web Services technology, to expose, use and combine government functionality implemented by public agencies. This paper presents the Uruguayan E-Government Platform focusing on two components of the Interoperability Platform: the Middleware Infrastructure and the Security System. It also evaluates its first years of operation which have shown that, although there are still many challenges to be addressed, the platform is a key enabler for developing a joined-up e-government approach in Uruguay.

Keywords: e-government, soa, interoperability, security, web services, middleware.

1 Introduction

During the last decades, Latin American countries have progressively been driving e-government initiatives. More precisely in Uruguay, the Electronic Government and Information Society Agency (AGESIC[1], Agencia de Gobierno Electrónico y Sociedad de la Información), which has the mission to lead the e-government strategy in Uruguay, aims to improve the services provided to Uruguayan citizens, leveraging the capabilities of Information and Communication Technologies (ICT). It also aims to

[1] http://www.agesic.gub.uy/

A. Kő et al. (Eds.): EGOVIS/EDEM 2012, LNCS 7452, pp. 140–154, 2012.

leverage, as far as possible, the existing available services in public agencies, which requires the integration of the information systems that implement them.

Similar to other regions, E-Government Platforms in Latin America have shown to be one of the key tools to support this kind of integration [1]. They usually provide infrastructure and services that facilitate the interconnection between the information systems of public agencies, provide common services that generate economy of scale, and encourage the implementation of multi-agency services.

In particular AGESIC has designed, built and made available the Uruguayan E-Government Platform [2]. This platform has the general goal of enabling and promoting the development of e-government services in Uruguay following a joined-up approach. The platform consists of an Interoperability Platform and a set of Crosscutting Services. The Interoperability Platform, which comprises a hardware and software infrastructure along with legal and technical frameworks, aims to facilitate the implementation of e-government services and their access. It also provides the support to implement a service-oriented architecture (SOA), where public agencies provide its government functionality through software services which are described, invoked and combined in a platform independent way.

This paper presents the Uruguayan E-Government Platform (EGP.uy), focusing on two of the components that support the Interoperability Platform: the Middleware Infrastructure and the Security System. The Middleware Infrastructure provides mechanisms to solve interoperability issues and to simplify the development, deployment and integration of services and applications within the platform. The Security System provides security services to the rest of the components and is the element in charge of the authorization, authentication and accounting (AAA) tasks in the platform. The paper also presents an evaluation of the first years of operation of the platform, describing its current situation and perspectives.

The rest of the paper is organized as follows. Section 2 provides background on e-government platforms and the Uruguayan e-government strategy. Section 3 presents a general overview of the EGP.uy. Section 4 describes the Interoperability Platform, in particular its Middleware Infrastructure and Security System. Section 5 presents the current situation and an overall evaluation of the EGP.uy. Finally, Section 6 presents conclusions and future work.

2 Background

This section presents background on the Uruguayan E-Government Strategy and related work on E-Government Platforms.

2.1 Uruguayan E-Government Strategy

In Uruguay, the e-government strategy has followed a joined-up approach based on an E-Government Platform (EGP).

The underlying context is characterized by a very heterogeneous application of IT in public services. While some public e-services have been developed since the year 2000, providing Web-based mechanisms to access information and/or to perform transactions, a large portion of public administration remains underdeveloped even for internal operations. Concerning the usage of Internet in households, Uruguay has very high rates. Furthermore, the IT industry is well developed and local professionals implement large-size systems using cutting-edge technologies like Web Services.

Based on this context, the main goals of the e-government strategy, which was developed in 2006, were to improve the quality of citizen services and the efficiency of public administration by promoting the implementation of IT-based services. More specifically, the e-government strategy aimed at facilitating public agencies to publish e-services, by providing them technical guidance and a large-scale infrastructure. While the technical guidance consists of defining IT standards and promoting a SOA application, the large-scale infrastructure consists of a high-quality communication network, a PKI system, and an Authentication System. The strategy also aimed at improving quality of service by involving private partners and by enhancing the efficiency of composed public-private services. The EGP constitutes, in this way, the key enabler of this nation-wide integration strategy. The extensibility of the approach is based on applying a standards-based modular approach to services, which enables new services to be added or changed with low impact. Finally, another objective of the e-government strategy has been to support the Open Data Government policy by offering a single access point through the portal services and several artifacts. This approach facilitates the implementation of this policy to all public agencies.

In summary, the strategy aimed at developing a joined-up approach by enabling the composition of services provided by public or private institutions, and therefore leveraging existing capabilities.

The adopted approach to carry out this strategy was mainly based on the implementation of an operational EGP, which is the cornerstone of the joined-up approach carried out in Uruguay. In order to strengthen the service integration and composition capabilities as well as the implementation of a SOA-based e-government, interoperability technologies are provided in all the EGP layers (e.g. business services through Web Services, user interaction through WSRP portals). To facilitate and speed up the implementation of such composed services, while atomic services execute on the agencies' servers, the core of the EGP was built using an advanced integration middleware. More concretely, an Enterprise Services Bus infrastructure was selected to provide these integration functionalities. Besides the e-government platform, technical specifications and standards were developed to provide guidance to agencies.

It is important to point out that the e-government strategy and the development of the EGP is part of a wider government policy (the Uruguayan Digital Agenda)[3].

2.2 Related Work on E-Government Platforms

In order to facilitate the execution of governmental processes and the interaction between the citizens and the governmental organizations, several countries all over the world initiate and conduct e-government initiatives [4].

To support them, countries follow different approaches, potentially complementary. Some approaches focus on defining frameworks which specify how to build e-government applications, but without providing an execution environment [5]. Others focus on providing EGPs [1][4][6][7], which usually comprises a technological infrastructure and services that supports the interconnection between Government Services. These platforms are usually based on standards to allow the integration between public agencies that may have different technological environments. Beyond their particular characteristics, EGPs usually provide a set of basic capabilities which include, among others, security, interoperability, connectivity and communication.

The distinct characteristic of the EGP.uy is that it focuses on building an open platform to promote the reuse of existing services running in public agencies. The main advantages of this approach are the intrinsic openness and extensibility of the platform, as well as the economy by promoting the reusability of existing solutions.

3 The Uruguayan E-Government Platform

The Uruguayan E-Government Platform (EGP.uy) has the general goal of facilitating and promoting the implementation of e-government services in Uruguay. To this end, the platform provides mechanisms which aim to simplify the integration between public agencies, to guarantee secure interactions within the platform and to allow the communication with citizens. This section provides a general overview of the platform, describing its main components, capabilities and actors.

3.1 General Description

The EGP.uy consists of an Interoperability Platform and a set of Crosscutting Services. The Interoperability Platform, which comprises a hardware and software infrastructure along with legal and technical frameworks, facilitates to public agencies the implementation of e-government services and their access. On the other side, the Crosscutting Services provides specific utilities to citizen and/or public agencies.

The technological support for the Interoperability Platform and the Crosscutting Services is given by various components which aim to simplify the integration between public agencies, assure that all interactions within the platform are performed in a secure environment and allow the communication with citizens. Fig. 1 presents these components, along with the main actors involved with the platform.

The components which support the Interoperability Platform are the Security System, the Metadata Management System and the Middleware Infrastructure. The Crosscutting Services are, at this time, the E-Government Portal, the Government Search Engine, the Electronic Record System and the Geographic Information Portal. Sections 3.2 and 3.3 present in more detail these components and services.

On the other side, the actors involved with the platform are the general public, public agencies and platform administrators. The general public (i.e. Uruguayan citizens, foreign people and private companies) accesses e-government services through the internet using, for example, the E-Government Portal or Web Services exposed at the EGP.uy. Public agencies leverage the connectivity provided by REDuy, a high-speed network infrastructure, to access and provide services and components in the EGP.uy. Finally, platform administrators deal with all the tasks concerned with the administration and operation of the platform.

REDuy [8] is a high-speed wide-area network which provides the required connectivity infrastructure to allow public agencies to access the EGP.uy and other agencies. REDuy is implemented over the MPLS (Multi Protocol Label Switching) network of ANTEL, the public telecommunications company of Uruguay, and it supports speeds from 10 Mbps to 100 Mbps. REDuy is protected by firewalls which control the network traffic, from and to the network.

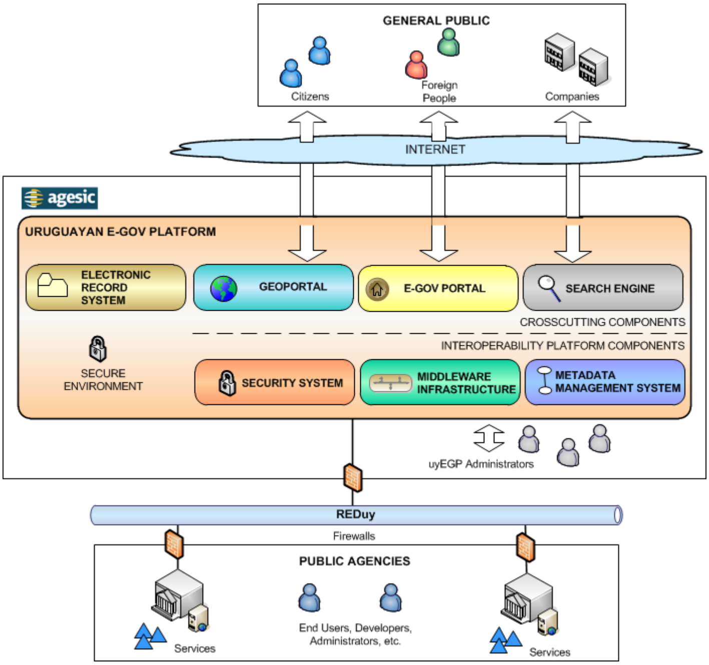

Fig. 1. Main Components and Actors of the EGP.uy [2]

The EGP.uy implements a SOA, leveraging the Web Services technology. In this way public agencies provide its government functionality through software services which are described, invoked and combined in a platform independent way. This aims to simplify the integration between public agencies, and to promote the reuse and exploitation of government assets. Additionally, it contributes to be able to respond in a more agile way to changes in requirements or regulations [9][10]. Software services provided by public agencies are usually hosted in servers located at the agencies. These services can be built from scratch or they can expose government functionality implemented in existing systems, leveraging in this way assets that the government already has. Additionally, if services have some special requirement that cannot be satisfied at the agencies, they can also be hosted at the EGP.uy.

It is important to remark that in order to support the use of the EGP.uy, now and for the future, a legal infrastructure had to be developed. This infrastructure comprises supporting laws and regulations regarding personal data protection, electronic signature (including advanced signatures), interoperability between public agencies and access to public information. There are currently other laws and regulations in process to be approved. It was also necessary to guide the adoption of several technological standards through guidelines and best practices. In order to use and publish services at the platform, public agencies must use this normative. This set of laws, regulations and technical recommendations are also part of the EGP.uy [11][12].

3.2 Crosscutting Services

At this time the Crosscutting Services are the E-Government Portal, the Government Search Engine, the Geographic Information Portal and the Electronic Record System.

The E-Government Portal[2] is the entry point to the Uruguayan government content and procedures available in the Internet [13]. The information included in the portal consists of headlines that are taken from different Uruguayan websites (mostly public agencies websites). Also, a link to the source website is included in each headline, so that citizens can access the complete content. This strategy contributes to improve the quality of information at the source, which is produced and managed by the public agencies themselves. The portal organizes and categorizes information, according to user profiles (e.g. women, students) and thematic areas (e.g. health, education).

From a technical point of view, the information from the source websites is integrated in the portal via RSS feeds hosted in the sites. If a website does not provide information in this format, screen-scrapping techniques are used to integrate the information in the portal. The implementation of the portal is mostly based on IBM WebSphere Portal and Lotus Web Content Management. The portal supports industry standards, like the Java Portlets specifications and Web Services for Remote Portlets (WSRP). Also, it complies with well-known web content accessibility guidelines.

The Government Search Engine[3] has the main goal of implementing a search engine oriented to the specific needs of the Uruguayan government. The main benefit, compared to using other general search engines like Google, is that it is optimized to search Uruguayan government content. The implementation of the search engine is based on Google Search Appliance (GSA) and SmartLogic Semaphore.

The GeoPortal[4] is a geographic information portal which allows querying and analyzing, through the Internet, the geographic information coming from public agencies. The Geoportal is one of the services in the Spatial Data Infrastructure project (IDE) which has the main goal of creating a network service to access and share geographic information across the Uruguayan public agencies. IDE services are compliant with the Open Geospatial Consortium standards[5].

The Electronic Record System has the goal of handling government records and simplifying their interoperability across public agencies. The main component of the system is an electronic record management application. This application can be used with a Software as a Service (SaaS) approach or can be installed in the public agencies themselves. Additionally, it will provide citizens with a Web interface which will allow them to trace records through the Internet.

3.3 Components of the Interoperability Platform

The Interoperability Platform facilitates the implementation of e-government services and their access. The components which support this platform are: the Metadata Management System, the Middleware Infrastructure and the Security System. The Metadata Management System provides a high level specification of the concepts related

[2] http://portal.gub.uy/

[3] http://buscador.gub.uy/

[4] http://idevisualizador.agesic.gub.uy/

[5] http://www.opengeospatial.org/

with public services in order to avoid, or even solve, ambiguities when public agencies use these concepts. The knowledge in this system is handled through ontologies specified via OWL (Web Ontology Language), using Protégé as the modeling tool. This system also exposes interfaces, through the Web Services technology, so that other systems can interact with it. The Middleware Infrastructure and the Security System are described in Section 4.1 and Section 4.2, respectively.

4 The Interoperability Platform

This section presents the main features provided by the Interoperability Platform, focusing on the Middleware Infrastructure and the Security System.

4.1 Middleware Infrastructure

The Middleware Infrastructure has the goal of promoting the interoperability between the different public agencies, providing the required mechanisms to facilitate the development, deployment and integration of application and services. These mechanisms are also the foundation to implement a SOA. The Middleware Infrastructure consists of three main blocks: execution environments, a Service Registry and ESB products.

Execution Environments. Even though applications and services provided by public agencies can be usually hosted at the agencies themselves, the Middleware Infrastructure provides execution environments to host them. These environments are based on commonly used middleware technologies, like application servers and ESBs.

Public agencies can leverage these environments to host applications and services which require advanced hardware and/or software infrastructure which, in some cases, is not available at the agencies. This infrastructure can be required to guarantee certain quality of service level regarding, for example, response time or availability.

Execution environments are also used to host application or services which provide general purpose functionalities or utilities. For example, there is a Timestamp service, provided by AGESIC, which returns the current date and time.

The Middleware Infrastructure provides execution environments for two of the main enterprise application platforms: Microsoft .Net Framework and Java Enterprise Edition (Java EE). The latter is provided through the JBoss Enterprise SOA Platform. This dual platform intends to face interoperability issues and provide technological independence in new acquisitions or developments. Moreover, the platform includes other advanced components, for example, WS-BPEL engines.

Service Registry. The Service Registry provides functionalities which allow publishing, describing, searching and discovering e-government services within the EGP.uy. In particular, the Service Registry provides all the required information, specified using the WSDL standard, to allow public agencies to invoke services. Besides this technical specification, when a public agency publishes a service in the EGP.uy, it has to specify additional information regarding quality of service (e.g. availability, response time and maximum throughput), security requirements (e.g. authorization mechanism), general documentation (e.g. description of operations and parameters, input and output examples), operational information (e.g. implementation language) and technical support information, among others. This information has to be specified in a service publication request form [14].

Although the Service Registry is currently an internal component within the EGP.uy (i.e. only AGESIC administrators can update it), AGESIC plans to provide a public Service Registry (e.g. an UDDI compliant registry) so public agencies can discover services by themselves.

Enterprise Service Bus Products. An Enterprise Service Bus (ESB) is a standards-based integration platform which includes different middleware technologies (e.g. message-oriented middleware and Web Services) and provides mediation capabilities (e.g. data transformation and intelligent routing) to reliably connect and coordinate the interaction of diverse applications in an heterogeneous environment [15]. When using an ESB, applications and services communicate by sending messages through the ESB. The Middleware Infrastructure includes two ESB products: JBoss ESB and Microsoft Biztalk Server (plus Biztalk ESB Toolkit). Some of the ESB features that are leveraged within the Interoperability Platform are location transparency, asynchronous messaging, message transformation and content-based routing.

Location transparency means that client applications are not aware of the real network address of the services they want to invoke. In order to invoke a service they have to specify a logical address which identifies services within the platform. The mapping between logical and real addresses is managed at ESB products. In this way, if a service changes its real address there is not any impact in client applications, given that the mapping can be adjusted at ESB products. Additionally, service providers (i.e. public agencies) do not need to make public the location of their servers, which contributes to achieve a higher security level for them. In the context of an invocation, the logical address of services is specified leveraging the WS-Addressing standard.

The Asynchronous Messaging capabilities allow supporting different messaging models. In particular, a publish-and-subscribe service was implemented to provide a broadcast-like communication mechanism where a producer notifies certain information to interested parties. The mechanism has two subscription modes: push and pull. Using the push mode, subscribers receive notifications in a specific service previously specified by them. Using the pull mode subscribers must communicate with the platform periodically to check if there is any new notification. The advantage of the push mode is a real time notification mechanism but requires a high availability infrastructure. On the other side, the pull mode has the disadvantage of receiving notifications on demand. Leveraging this publish-and-subscribe mechanism, a service which notifies changes in citizen's data (e.g. marital status) was implemented.

The Message Transformation capabilities allow transforming messages passing through the ESB according to a given transformation logic specified, for example, using XSLT. In the context of the Interoperability Platform, this capability has been used to solve different interoperability problems, given that although the interactions between public agencies are based on Web Services standards, this is not always enough to guarantee end-to-end interoperability [16]. Transformations can also be used to reduce the impact in client applications when a service contract changes [17].

The Content Based Routing capability routes ESB messages according to the messages content. It is used within the platform to route messages to the real address of services: it obtains the logical address of the service from the WS-Addressing header, gets the real address from a mapping table and routes the message to this address.

4.2 Security System

The Security System provides the mechanisms to enforce AAA policies according to the security requirements of the applications, services or components in the EGP.uy. Public agencies can delegate the compliance with Web Services' security requirements to this component. The Security System can be divided in three main blocks: the Audit System, Peripheral Security Services and the Access Control System.

Audit System. The Audit System provides the required tools to perform security audits in the EGP.uy. The system gathers information and performs audit analysis and reports that can answer questions such as, among others, who consumed this service?, and at what time?. The Audit System is based on Tivoli Compliance Insight Manager.

Peripheral Security Services. The Peripheral Security Services have the main goal of facilitating the secure access of public agencies to the EGP.uy and comprise two main services: a Certification Authority and a Directory Service.

The Certification Autority (CA) has the goal of issuing and managing the general purpose digital certificates that are used within the platform. For example, the CA issues the certificates which are used by the servers to establish secure connections with the EGP.uy. The implementation of the CA is based on Windows Server 2003.

The Directory Service provides directory services through the LDAP protocol and has four main functions [2]: i) replicate, in an automatic way, the directory structures of the public agencies that have a directory service, ii) provide directory services for applications deployed within the EGP.uy, iii) provide directory services to public agencies which do not have one, and iv) provide a unified view of the government directory structures. The Directory Service is mainly implemented with IBM Directory Server, Tivoli Identity Manager and Tivoli Directory Integrator.

Access Control System. The goal of the Access Control System is to provide mechanisms that allow applying access control policies over application and services available within the EGP.uy. These mechanisms follow a Role Based Access Control (RBAC) schema. The Access Control System has three components: the Security Token Service, the Security Policy Manager and the XML Firewall.

The Security Token Service (STS) has the responsibility to issue the required security tokens to allow client applications to invoke services published in the EGP.uy. This component is compliant with the WS-Trust v1.3 standard and it is based on Tivoli Federated Identity Manager. The STS trusts the authentications performed at the public agencies to issue security tokens. In particular, it verifies the authenticity of the requests through digital signature mechanisms.

When an application running in a public agency wants to invoke a service in the EGP.uy, it first has to request a security token to the STS. This request is performed using the WS-Trust standard and includes a security token, specifying the user role invoking the service. The security token is specified using SAML (v1.1 or v2.0) and it is digitally signed by the public agency. When the EGP.uy receives a security token request, it verifies the digital signature of the token included in the request. It also verifies that the user role specified in the security token is in the LDAP directory. If all the verifications succeed, the STS issues a security token, including the user role, which is specified using SAML v1.1 and is digitally signed by the EGP.uy. The communication between public agencies and the STS is performed over HTTPS.

The Security Policy Manager acts as a Policy Decision Point (PDP), given that it is in charge of authorizing the requests for invoking services in the EGP.uy. To this end, it stores information about which roles have access to which operations of the published services. When the EGP.uy receives a request (i.e. a SOAP message) to invoke an operation of a given service, it obtains from the WS-Addressing headers the logical address of the service and the operation to be invoked. It also gets the user role from the security token which is included in the message following the WS-Security standard. In this way, it has all the required information (service, operation and role) to be able to authorize, or not, a given invocation request. The Security Policy Manager is implemented with Tivoli Security Policy Manager.

The XML Firewall acts as Policy Enforcement Point (PEP) leveraging the decisions taken by the Security Policy Manager. For each service published in the EGP.uy, a proxy service is deployed in the firewall. When a client application wants to invoke a service, the invocation has to be done through its proxy service. In case the firewall authorizes the invocation, it routes the request to the Middleware Infrastructure which finally sends the request to the service. Otherwise, an error message is returned to the client application. These interactions are also performed over HTTPS. The XML Firewall is implemented with IBM Websphere Datapower Xi50.

4.3 Steps in a Service Invocation

Fig. 2 presents a summary of the required steps to perform a service invocation within the EGP.uy, focusing on the processing at the Interoperability Platform.

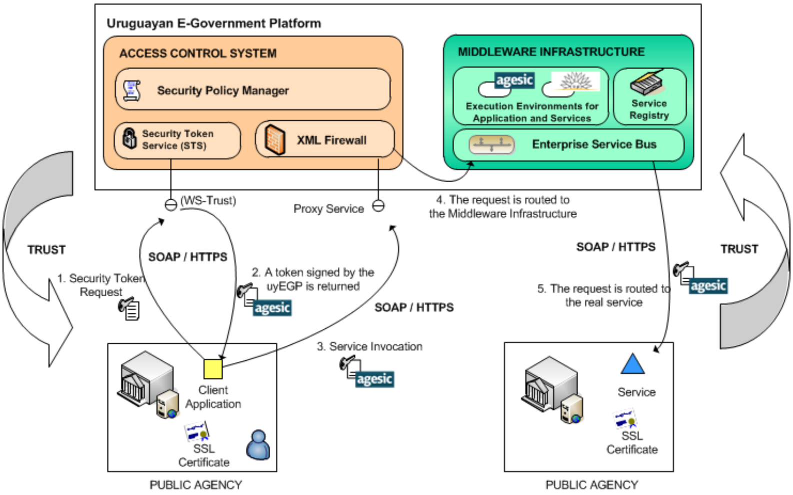
Uruguayan E-Government Platform
ACCESS CONTROL SYSTEM
Security Policy Manager
Security Token Service (STS)
XML Firewall
MIDDLEWARE INFRASTRUCTURE
agesic
Execution Environments for Application and Services
Service Registry
Enterprise Service Bus
(WS-Trust)
Proxy Service
4. The request is routed to the Middleware Infrastructure
TRUST
SOAP / HTTPS
1. Security Token Request
2. A token signed by the uyEGP is returned
agesic
SOAP / HTTPS
SOAP / HTTPS
5. The request is routed to the real service
agesic
TRUST
3. Service Invocation
agesic
Client Application
SSL Certificate
PUBLIC AGENCY
Service
SSL Certificate
PUBLIC AGENCY

Fig. 2. Service Invocation [2]

4.4 Summary of Features Provided by the Interoperability Platform

As presented in previous sections, the Interoperability Platform provides different features that public agencies can leverage. The implementation of these features at the Interoperability Platform generates economy of scale, given that with a single effort various agencies can be benefited.

Additionally, the capabilities provided by the Interoperability Platform allow implementing other mechanisms to deal with specific requirements that public agencies might have. In particular, some mechanisms were implemented in the platform to control the number of invocations of a service according to different factors.

The load control mechanism limits the number of invocations per second a given service can have. In turn, the time control mechanism restricts the times of the day in which a service can be invoked and, in these periods of time, it also limits the number of service invocations per client. Finally, the date control mechanism controls that services can be invoked in specific dates.

As a summary, the Interoperability Platform offers these main features to public agencies: i) execution environments, ii) synchronic service invocation, iii) publish and subscribe service, iv) access control mechanisms, v) directory service (LDAP), vi) security audit services, and vii) load, time and date control for service invocations.

5 Current Situation and Evaluation

Since its start-up in 2009, public agencies have been progressively joining the EGP.uy. This section describes its current situation and presents a general evaluation.

5.1 Current Situation

About 150 nodes, belonging to different agencies, are currently connected to the RED.uy and other 20 are expected to join it in the short term. In addition, several services and applications, like Web Services, Portal and government business applications, are already accessible through the REDuy. The Interoperability Platform currently publishes twenty three services; ten of them implement public administrative procedures while the others correspond to internal interactions between public agencies. One example of implemented administrative procedures is the Electronic Certificate of Decease, which enables authorized users to access the certificates issued in a given period of time. Another example is the Basic Identification Service, which enables to obtain personal data of a citizen (e.g. names, sex and birthday) given the national identification number. These services are currently used by nine different agencies. For example, the Social Development Ministry, which administers social programmes to assist low income population, uses the Basic Identification Service to validate the identity of the beneficiaries of the programmes. Currently, there are also more than twenty services in testing phase.

Concerning the performance of the published services, monitoring have shown that invoking a service through the platform (i.e. the steps in Fig. 2) has an overhead of, at most, one second more than point-to-point invocations between agencies.

5.2 Main Benefits

While the most evident benefit of the EGP.uy is to provide a legal and technical framework that can be used by public agencies to collaborate and reuse existing information and services, there are other economic, administrative and development ones. The EGP.uy design (a broker between all the agencies using standardized protocols) enables to reduce point-to-point agreements between agencies as well as their associated burden (e.g. definition of exchange protocols and formats). This has also enabled to reduce costs and software development workload as well as reducing barriers for incorporating advanced integration technologies. Furthermore, the standards and good practices promoted by the EGP.uy helped agencies to achieve higher quality implementations than former ones based on legacy technologies.

From a legal point of view, the EGP.uy enables to ensure that information exchanges comply with Uruguayan laws and regulations (e.g. personal data protection). From an economic point of view, the EGP.uy aims at promoting economy of scale by providing applications and services that can be reused by several agencies. From an administrative point of view, the EGP.uy provides a centralized Service Registry which constitutes the basis of the e-Government SOA Governance. This Registry provides rich information for each service including documentation, QoS information (response time and max throughput), technical and business contacts and technical issues support. AGESIC also provides assistance to agencies that do not find services matching their requirements.

Concerning application development using the platform, AGESIC provides a first level of technical support. Developers do not interact with products' support services but with AGESIC support team, which assist them on dealing with integration requirements (SSL, Certificates, Web Services, etc).

Finally, the design of the EGP.uy, based on an open service approach in which any agency can publish and consume services, promotes the development of new services by composing existing ones.

5.3 Main Challenges

Public agencies joining the EGP.uy generally face technical and cultural challenges. While technical problems (e.g. interoperability issues, inadequate hardware or software infrastructures, etc) are usually solved in the first phase of the integration process, cultural ones are harder to address and they can have a negative impact in the success of the integration [18]. In particular, the resistance to use EGP.uy because it is external to agencies and the seizure of information have been the most common cultural problems. Furthermore, the lack of confidence in the platform, for example regarding security, performance and availability, were also important barriers. The first generation of services, although very basic and with limited business value and reuse, enabled agencies to better understand the EGP.uy. After this initial phase, new generations of more valuable and sophisticated services have been implemented.

Finally, it took time to public agencies to "take possession" of the EGP.uy and consider it as part of their IT commodities.

All this difficulties are being addressed through different initiatives like workshops focusing on the usage of the platform, guides and tutorials, software components that simplify the integration with the EGP.uy and training courses along the year. These initiatives have been well received by agencies and have apparently paid off, as the number of new services in the first quarter of 2012 is the same than the number of new services throughout 2011.

5.4 Lessons Learned

The three years process of development and operation of the EGP.uy enable to summarize some main lessons: i) training IT staffs in agencies, providing technical support and assistance, and developing adapters and libraries that simplify the integration to the platform had a key impact in reducing the technological gap between agencies and the EGP.uy, ii) in order to use the platform, public agencies have had to understand the benefits of the EGP.uy; developing an effective communication and joined work with the agencies enabled to generate this knowledge and trust, iii) when agencies received additional benefits for publishing/consuming services they were much more motivated to use the platform, iv) involving operational IT staff from the beginning promoted the appropriation of the EGP.uy and made them to feel that is part of their IT infrastructure, and v) developing new common solutions based on agencies' requirements have been a key type of activity to address complex applications.

6 Conclusions and Future Work

This paper presented the design, architecture and implementation of a joined-up e-government approach based on an advanced middleware platform.

This experience has shown the feasibility of implementing an EGP using state of the art technologies, especially middleware and security, and the potential of a middleware-based integration platform to support a large variety of value-added services. The E-Government program also enabled improving the overall AGESIC technological services (e.g. the National Root PKI, Network Time Services). Finally, the current increased demand for services shows that this is a midterm investment. On the other side, technical and cultural challenges still remain, which can constitute barriers for a successful integration with the platform.

The main contributions of the paper are the technical description and evaluation of the approach followed in Uruguay, which is based on an integration platform promoting reuse and composition of services running in public agencies. Furthermore, the paper explains the key role of the ESB as integration middleware. Finally, the paper could enable to evaluate the followed approach to implement an e-Government strategy centered on reusing and composing existing services.

Future work involves three groups of initiatives: new services for citizens and public agencies, enhancement of the EGP.uy and enhancement of some platform services. The initiatives in the first group are to: i) frameworks to support online transactions through reusable components (e.g. electronic forms), ii) Government Resource Planning services, and iii) e-health services (e.g. medical terminology services, HL7 broker, telehealth services). The initiatives in the second group are Integrating

Geographic Services with the Interoperability Platform [19], developing adaptive ESB mechanisms to deal with quality of service [20][21], and perform automatic regulatory compliance validations (e.g. regarding Personal Data Protection). Finally, the initiatives in the third group are supporting file exchange over the EGP.uy, enhancement some security topics like citizen authentication (end-to-end security), enforce security at the message level (e.g. integrity) and supporting multi-agency service compositions.

References

1. Items International, Moreno Escobar, H.: CEPAL - e-Government architectures, technical and political situation in Latin America, http://www.eclac.org/ddpe/publicaciones/xml/7/28647/W129.pdf
2. AGESIC - Guía de uso de la Plataforma de GE del Estado uruguayo, http://www.agesic.gub.uy/innovaportal/v/1454/1/agesic/guia_de_uso_de_la_plataforma_de_ge_del_estado_uruguayo.html
3. AGESIC - Agenda Digital Uruguay 2011 - 2015, http://www.agesic.gub.uy/innovaportal/file/1443/1/agesic_agendadigital_2011_2015.pdf
4. Helali, R., Achour, I., Labed Jilani, L., Ben Ghezala, H.: A Study of E-Government Architectures. In: Babin, G., Stanoevska-Slabeva, K., Kropf, P. (eds.) MCETECH 2011. LNBIP, vol. 78, pp. 158–172. Springer, Heidelberg (2011)
5. Interoperability Solutions for European Public Administrations - ISA - European Commission, http://ec.europa.eu/isa/index_en.html
6. Batini, C., Cappadozzi, E., Mecella, M., Talamo, M.: Cooperative Architectures - The Italian Way Along e-Government (2002)
7. Sudoh, O., Kinoshita, Y.: Transformative and Innovative E-Gov for the Next Generation: Linkages of Back Offices for One-Stop Portal. In: Janssen, M., Lamersdorf, W., Pries-Heje, J., Rosemann, M. (eds.) EGES/GISP 2010. IFIP, vol. 334, pp. 111–124. Springer, Heidelberg (2010)
8. AGESIC - REDuy, http://www.agesic.gub.uy/innovaportal/v/759/1/agesic/REDuy.html
9. Practical Guide to Federal Service Oriented Architecture | The White House, http://www.whitehouse.gov/omb/E-Gov/pgfsoa
10. Papazoglou, M.P., Traverso, P., Dustdar, S., Leymann, F.: Service-Oriented Computing: State of the Art and Research Challenges. Computer 40, 38–45 (2007)
11. AGESIC - Marco legal, http://www.agesic.gub.uy/innovaportal/v/42/1/agesic/marco_legal.html
12. AGESIC - Normas Técnicas, http://www.agesic.gub.uy/innovaportal/v/114/1/agesic/normas_tecnicas.html
13. AGESIC - Portal y Buscador del Estado, http://www.agesic.gub.uy/innovaportal/v/1067/1/agesic/portal_y_buscador_del_estado.html
14. AGESIC - Formulario de Solicitud de Publicación de Servicio en la PGE, http://www.agesic.gub.uy/innovaportal/file/1929/1/formulario_solicitud_publicacion_servicios_pge_v2.4.odt

15. Chappell, D.: Enterprise Service Bus: Theory in Practice. O'Reilly Media (2004)
16. Lewis, G.A., Morris, E., Simanta, S., Wrage, L.: Why Standards Are Not Enough to Guarantee End-to-End Interoperability. In: Seventh International Conference on Composition-Based Software Systems (ICCBSS 2008), Madrid, Spain, pp. 164–173 (2008)
17. González, L., Ruggia, R.: Addressing the Dynamics of Services Contracts through an Adaptive ESB Infrastructure. Presented at the 1st International Workshop on Adaptive Services for the Future Internet
18. Jimenez, C.E., Criado, J.I., Gasco, M.: Technological e-Government Interoperability. An Analysis of IberoAmerican Countries. IEEE Latin America Transactions (Revista IEEE America Latina) 9, 1112–1117 (2011)
19. Sosa, R.: Integración de Servicios Geográficos en Plataformas de Gobierno Electrónico (2011)
20. González, L.: Plataforma ESB Adaptativa para Sistemas Basados en Servicios (2011)
21. González, L., Ruggia, R.: Addressing QoS issues in service based systems through an adaptive ESB infrastructure. In: Proceedings of the 6th Workshop on Middleware for Service Oriented Computing - MW4SOC 2011, Lisbon, Portugal, pp. 1–7 (2011)