# Processes Traceability in the State


## ABSTRACT

The evolution of the Electronic Government has led to the digitization of several processes in the State. These processes, implemented using different tools and technologies have difficulties when are going to be audited or when their status has to be provided. In order to solve these problems and provide transparency in government a system for the traceability of processes was built. Any cross-cutting solution in Uruguay has to be part of the Uruguayan e-Government Platform (PGE in Spanish) and to uses the Interoperability Platform (PDI in Spanish) as a switching point between institutions. This paper describes the architecture of the solution for the traceability of processes and the fundamental role played by the interoperability platform, facilitating integration.



## Categories and Subject Descriptors

A.0 **[General]**: Conference proceedings

## General Terms

Measurement, Performance, Design, Reliability, Standardization, Legal Aspects

## Keywords

Traceability, Interoperability, e-Government, Platform, Transparency


## 1. INTRODUCTION

In 2009 the Uruguayan Electronic Government Platform was developed, having the E-dossier as the first cross-cutting solution. This solution was accompanied by the definition of a standard for exchanging electronic files between agencies to resolve the interoperability of heterogeneous solutions at the semantic level.

The implementation of the exchange solution, Application of routing and traceability for electronic dossiers (ARTEE in Spanish) had two main components: one for routing of dossiers and another for the traceability. The first was aimed to solve the technical interoperability, while the second aimed to record every transaction and the status of the dossiers. The intention was to achieve audit controls, obtaining metrics of the dossiers and to inform their status.

Based on the idea of the dossiers traceability, in late 2014 different solutions for traceability of generic Government processes were studied.

The solution had to have the same purpose as the traceability of dossiers, but with the difference that the system should also allow the display of information of certain processes to the citizens, thus contributing with the process transparency.

Throughout this document context application of the traceability solution, its architecture and coming steps will be presented.



## 2. SOLUTION CONTEXT

### 2.1 Processes in the State

The contextualization of processes in the State has a clear problem of disparity in the scope and execution domain. These go from financial and economic processes, welfare and safety processes, even to health-related processes.

The implementation suffers from the same problem as the contextualization. Some processes are already digitalized, but many of them don't. Also, digitized processes have very different solutions in terms of technology and design. All these issues put the implementation of the process audit, measurement, control and communication solution in a very complex situation.

In the past there have been projects aimed at optimizing and digitizing of processes where multiple agencies were involved. Thus arose projects such as "Company in a day", which provides a one-stop-shop where formalities to create enterprises can be made in the same place and time. Another example is one-stop-shop for foreign trade (VUCE in Spanish), who concentrates most of the customs' processes in a single point of contact. While both cases are examples of success stories in terms of process optimization and governance, each one has its own audit and control mechanisms.

However, the emergence of formalities optimization projects, such as "Simplificación de Tramites" in 2012 and more recently Online Formalities (Trámites en Línea in Spanish), has contributed in the provision of a more comprehensive and standardized view of the processes involved. Their concept includes processes with varied domains, with a large set of organizations involved and with direct impact on citizens.

These features provide an ideal scenario for the design of a standard solution for processes optimization which allows above-mentioned auditing and control features.

### 2.2 Online Formalities

The Online Formalities program aims to digitize all procedures that citizens and companies have to make with the State, in order to simplify interactions and improve services. Starting from a heterogeneous scenario of formalities´ processes, it was decided to work in a model that would allow digitalization with the least impact and in a non intrusive manner.

During 2012, AGESIC worked on a model to simplify formalities. This model represents the basic steps that all formalities must comply. This includes, for example, the initial step to begin a formality, the user identification, interoperability solutions, electronic communication and notification among the actors. From this concept model emerged a set of technology components that supported the technical implementation of the solution. The first's ones to be worked were the user identification and the notification solution

During 2014, the course of the project focused more at the initial step to begin a formality, considering the goal set by the President: By 2016, all formalities will be able to be initiated and also tracked by Internet and mobile devices, including payment options.

This implies the need of having auditing mechanisms for the transactions, for a volume of about 1,300 formalities distributed across the State, and giving visibility and transparency to the public at the same time.

## 2.3 Traceability of formalities

In order to meet the requirements of audit, control and communication of the formalities, in 2015 the design and implementation of a solution for their traceability was began. These tasks were part of a project called Traceability (Trazabilidad in Spanish) which is part of the Online Formalities program.

In this context, the main objectives for the project implementation were:

- All formalities should be traceable.
- All agencies must be able to generate traces, no matter if their formalities are digitized or not.
- The technological solution must be easily accessible for the agencies and the least intrusive possible.
- The traces must allow having information about the various steps involved in a formality, including its current status.
- Information on the status should be providing to citizens and businesses.

These objectives were the inputs used to work first on a generic architecture solution, and then for the technological and conceptual implementation of the traceability solution.

# 3. TRACEABILITY ARCHITECTURE

As every cross-cutting solution, the Traceability solution must run using the Uruguayan e-Government Platform. This allows having a set of basic functionalities such as:

- Physical layer connectivity with the different actors of the State
- Interoperability by standard mechanisms between state agencies
- Transaction level security (authentication, authorization and auditing of transactions)
- Message Routing and ability to perform transformations
- Authentication of users through Single Sign On system
- Privacy and data protection
- Ability to communicate to citizens and businesses (State Portal)
- Monitoring and management tools

This set of functionalities simplifies the process of defining the architecture as well as the technological implementation of the solution.

## 3.1 Uruguayan e-Government Platform

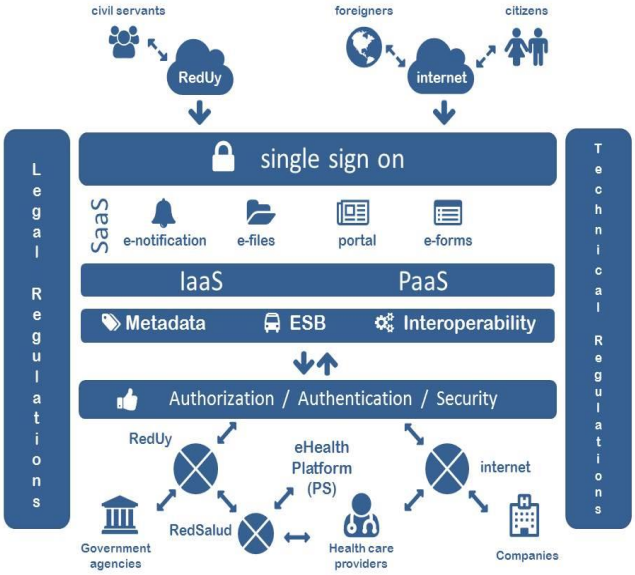


**Figure 1.e-Government Platform .**

The Uruguayan e-Government Platform is divided in two logical layers and a physical one. The physical layer is a Cloud, known as the Presidential Cloud, which delivers services as: Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). This implementation offers an infrastructure strategy that optimizes the resources and at the same time simplifies the management and governance. The logic layers are the Interoperability Platform and the Crossed applications. The Interoperability Platform is the implementation of the integration service strategy for backend systems, while the Crossed Application layer is the implementation of the Software as a Service (SaaS) layer of the Cloud.

### *3.1.1 Crossed applications*

The Crossed Application layer platform has two sublayers, an Application layer and a security layer. The Application layer is in charge of holding all applications of common use across the Government. Some of them are the e-Dossier solution, the Uruguayan Citizens Portal the e-Notification solution. The security layer delivers security services for all applications deployed in the Application layer, as well as a Single Sign On (SSO) solution for applications hosted in other State agencies. The SSO solution is based on a federated identity schema across the Government, with a centralized authentication on the PGE and a distributed authorization on each solution. The authentication is handled with SAML 2.0 tokens over HTTP headers, which allows an easy and standard way of integration.

### *3.1.2 Interoperability Platform*

The PDI integrates systems across the state in a backend level. It is divided in two layers: an interoperability layer (semantic and technical) and a security layer. The semantic Interoperability is solved by the metadata definition of common objects. Those definitions are made in agreemen with all agencies involved in the use of that information and published in the form of a data dictionary, an xml schema and an uml object diagram. The technical interoperability is implemented with an Enterprise Service Bus (ESB) acompained of a set of definitions based in

open standards. This allows the simplification of data exchange and the ability of offering added value services on it. All exchanges over the platform are based on Web Services Soap1.1 and complies with WS-Basic Profile 1.1. Message delivery is implemented using WS-Addressing standard, which provides capacity of dinamyc routing. The security layer covers phisical security and logical security. SSL v3.0 (HTTPS) with mutual authentication is used for the phisical transpor security. Logical security covers authentication and authotization of services. This is carried out by SAML1.1 tokens, which are exchanged with the platform using WS-Trust and WS-Security standards. In order to ensure tokens authenticity, E-signature through certificates X.509 v3 is used. Comunications within security components is held by the use of XACML 2.0. Open standards allow universal use of the platform, becoming independent from proprietary protocols and overcoming difficulties at the integration stage.

### *3.1.3 e-Government Platform "plug"*

The PGE plug (Conector in Spanish) is a black box software designed to facilitate the use of web services through the Interoperability Platform. The plug runs within the client infrastructure and basically its purpose is to act as a proxy for invoking services through the PDI.

Thus, end customers have the possibility to invoke the service through the plug (which does not define security features). In a transparent manner the plug enrich the message with the requirements and standards set by the Platform (WS- Trust, SAML, WS-Addressing, SSL with mutual authentication).

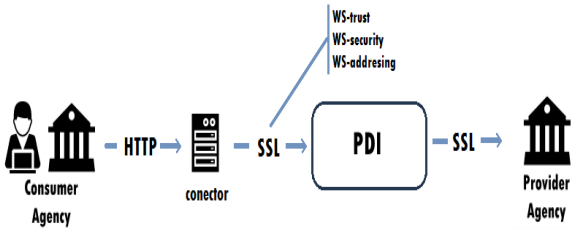


**Figure 2.e-Government Platform "plug"**

## 3.2 Traceability solution

The design of the traceability solution consists of two artifacts: the solution architecture and the semantics of the traces. By separating the semantic definition from the solution architecture it is achieved a decoupled implementation from the data transferred.

This allows that possible changes in the metadata do not affect the mechanisms of sending, receiving and viewing traces.

### *3.2.1 Architecture of the Traceability*

When defining the architecture, two problems were detected:

- Sending and receiving of traces.
- After obtaining the traces, to be able to visualize and communicate information about the formalities.

#### *3.2.1.1 Trace Sending*

The sending of traces was conceived as a hybrid scheme in which agencies send traces to a centralized repository, and be able to have its local records. This scheme provides the flexibility to send traces synchronously or asynchronously, persisting or not in its local environment, without having an impact on its flow or in its processing capability.

Even the system is flexible; the prompt dispatch of the traces is promoted. In order to measure this, a scheme of reliability was defined, which takes the time elapsed between the occurrence of the event that generates a trace and its sending. This measurement allows to take corrective actions in cases of delay and to identify possible improvements in the agencies systems.

It is important that this solution is agnostic to the content of the traces, so no integrity controls or corrections are made during reception.

The corresponding interactions when sending a trace to the back-end of the traceability solution, take place through the Interoperability Platform using SOAP Web Services. This simplifies the transportation, the security, the auditing and standardization, while allowing to offer value-added services if necessary.

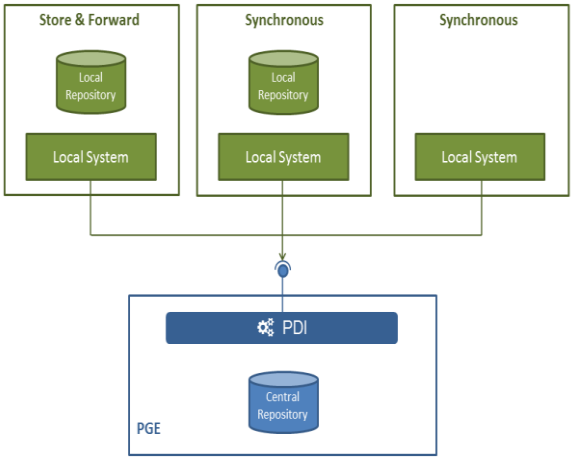


**Figure 3.Trace sending hybrid schema.**

Also, the use of the Interoperability Platform allows agencies, without digitized processes, to send their traces manually. This is accomplished through the use of the "Conector" and a component called "Web Interfaces". This component takes the WSDL and schemas associated to a service and generate a web form that can be completed manually. Then the information can be sent as web service. This component used for traceability services, ensures the possibility of sending traces manually.

#### *3.2.1.2 Visualization of the traces*

The implemented solution for the visualization is feed by the traces that the agencies send and that are stored at the centralized repository. Since at the time of receipt the consistency controls are not performed, it is necessary to normalize the data before viewing.

To achieve this goal, a normalized repository of traces was created. This is feed by a set of processes that run over the centralized repository and that standardizes and validates the quality of the traces.

The visualization for the citizens is done by accessing a portlet that will be published on site tramites.gub.uy. This porlet is able

to access to the information by calling a service published at the back-end of the traceability solution.

In the case of civil servants, a Web application to access consultations status and statistical reports on their transactions will be provided. This application accesses the information in the same way that the citizens Porlet, invoking services published at the back-end of the traceability solution.

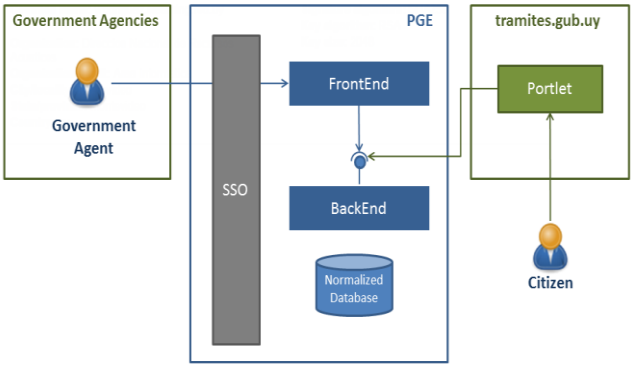


**Figure 4.Trace Visualization.**

### *3.2.2 Semantic of the trace*

The definition of the trace semantics assumes that it has to be self contained. This means that seeing a trace can show the process it refers and its status, in addition to obtaining its specific metadata.

The content of the trace is split into two sections, a fixed head and a line. All traces of a step of a formality share a fixed head and add a variable line with the specific information about the status. This scheme allows the correlation of traces from a same formality from the information thereof even allowing that traces arrive in different order. Over the head of each trace travels important data for the identification of the formality (process type, process ID and transaction ID), for correlating the traces (identifier of the "Father" transaction and of the step in the process execution) and for visualization. This correlation is done by the inclusion of a unique identifier that is assigned to each instance of the process, which is the same that citizens and public servants uses to visualize the status.

## 4. CURRENT STATUS AND COMING STEPS

Currently the solution is at an advanced stage of development, willing to be completed by the end of 2015. The put production deployment will be in the first quarter of 2016, in order to accompany the Online Services program.

In parallel with the development of the solution, AGESIC is working on designing a solution to start a new formality as a step of an initiated process or formality; even both processes belong to different government agencies. This involves the transfer of context information of the formality, including the head of the trace of the original one.

Regarding the next steps of the traceability solution, AGESIC will work on the implementation of the "Store and Forward" pattern over the “Conector”. This aims to solve on each agency the logic of storing in a local repository and sending traces.

Finally, once the system is in use, it will be taken measures in order to detect patterns and behaviors. Those will be used to predict ending times for processes, remaining steps and automated alerts.

## 5. REFERENCES


[1] AGESIC. Evolución tramites.gub.uy 2013. http://www.agesic.gub.uy/innovaportal/v/3096/1/agesic/evolucion-tramitesgubuy-2013.html

[2] AGESIC. Expediente Electrónico. http://www.agesic.gub.uy/innovaportal/v/3910/1/agesic/expediente-electronico.html?idPadre=4047

[3] AGESIC. Plataforma de Interoperabilidad. http://www.agesic.gub.uy/innovaportal/v/3922/1/agesic/plataforma-de-interoperabilidad.html?idPadre=4048

[4] AGESIC. PGE-Connector. http://www.agesic.gub.uy/innovaportal/v/2817/11/agesic/conector_pge.html

[5] AGESIC. Technical standards and best practices. http://www.agesic.gub.uy/innovaportal/v/114/1/agesic/Normas-Tecnicas.html

[6] OASIS. Web Services standards. https://www.oasis-open.org/standards