Plataforma de Interoperabilidad

Plataforma de Interoperabilidad I: Consumo de servicios

Control de Cambios

Fecha	Versión	Responsable	Cambios
	1.0		Versión inicial
19/09/2016	11.0		

Plataforma de Interoperabilidad

Versión 1.0 – 2015

Contenido

Introducción 4
¿Qué es la Plataforma de Interoperabilidad? 4
REDuy 6
Plataforma de Interoperabilidad 6
Principales beneficios 6
Estandarización y reducción de costos 6
Diseño SOA (Service Oriented Architecture) 7
Principales características 7
Componentes de la PDI 9
Catálogo de servicios 10
Consumo de servicios 11
Servicios de seguridad 11
Proceso de WS – Trust + SAML 12
Certificados 13
Servicio de ruteo 14
Escenario de Consumo de servicios en PDI 16
Descripción del escenario 16
Modalidad para consumir un servicio 18
Conector PGE 20
Reportes 21

Introducción

¿Qué es la Plataforma de Interoperabilidad?

La Plataforma de Interoperabilidad (PDI) forma parte de la Plataforma de Gobierno Electrónico (PGE) de AGESIC y tiene como objetivo general facilitar y promover la implementación de servicios de Gobierno Electrónico en Uruguay. Para esto, la PDI brinda mecanismos que apuntan a simplificar la integración entre los organismos del Estado y a posibilitar un mejor aprovechamiento de sus activos.

A nivel tecnológico, la PDI posibilita que distintos organismos publiquen procesos de negocio a través de servicios web, independientemente de la tecnología en la que éstos se encuentren desarrollados. La Arquitectura orientada a servicios (SOA) que implementa la PDI permite que distintos organismos del Estado puedan incorporar de manera estándar funcionalidades de negocio que ya se encuentran desarrolladas y publicadas por otros organismos estatales. Esto lleva a una reducción de tiempos de desarrollo, costos, y duplicidad de la información, entre otros.

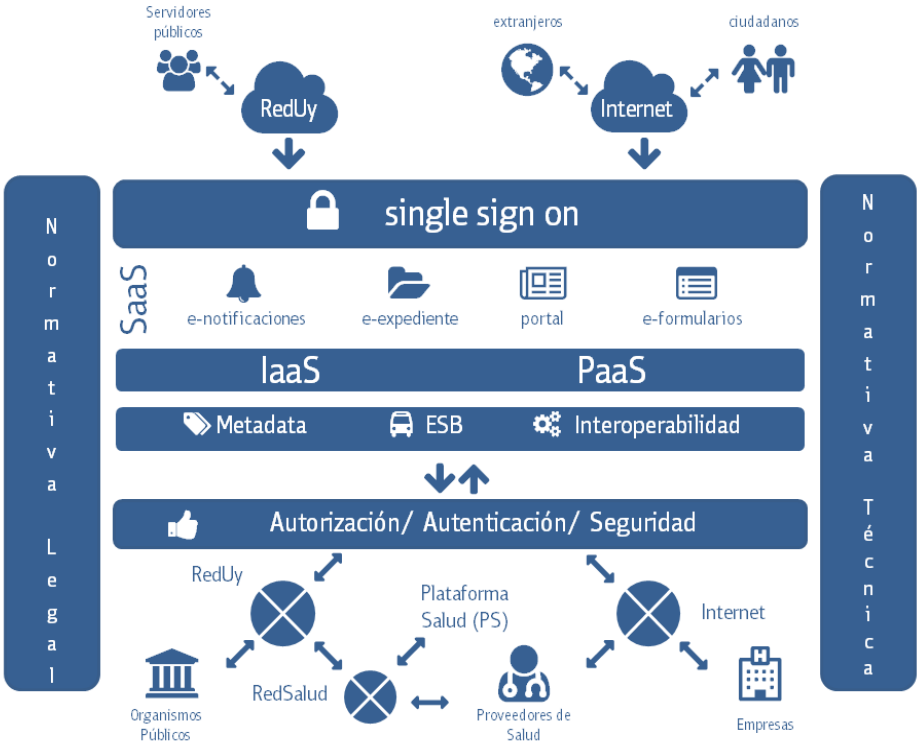

Ilustración 1 - PGE

La integración de sistemas del Estado a través de la PDI promueve la integración de procesos de negocios de los distintos organismos, y como consecuencia se reduce la cantidad de pasos que un ciudadano tiene que ejecutar al momento de realizar un trámite estatal en determinado Organismo. El objetivo final es no pedirle al ciudadano información que el Estado, como un todo, ya posee.

La Plataforma de Interoperabilidad brinda un marco legal y técnico a todas las transacciones que por allí pasan. A su vez, establece un único punto de acceso hacia los servicios que son expuestos a través de ella, y todas las comunicaciones son a través de una red privada y de alta velocidad llamada REDuy.

Tres grandes sistemas son los que conforman la PDI:

Ilustración 2 Definición de PDI

El **sistema de control de acceso**, integrado por una suite de productos que permiten la autenticación y autorización para el consumo de servicios basados en XML, oficia de puerta de entrada a la Plataforma.

El **sistema de gestión de metadatos** provee una especificación de alto nivel de los conceptos relativos a servicios públicos, de forma de evitar, o eventualmente resolver, ambigüedades en el manejo de estos conceptos por parte de los organismos.

Finalmente, el **componente de middleware** de la PDI cuenta con mecanismos para facilitar el desarrollo, despliegue e integración de servicios y aplicaciones. Los organismos pueden utilizar esta plataforma para publicar y descubrir servicios, así como utilizar las diferentes capacidades de mediación, las cuales permiten desacoplar clientes y servicios.

REDuy

La REDuy es una red de alta velocidad de fibra óptica, diseñada y desplegada como una Intranet del Estado uruguayo. La arquitectura de la red genera una malla (todos interconectados con todos) sin la necesidad de tener enlaces punto a punto. Es decir, cada organismo está interconectado con todos los demás solo con un enlace, con ancho de banda de 10 Mbps o 100Mbps. Se trata de una red privada y segura, que cuenta con la supervisión y el control expresos del CERTuy (Centro de Respuesta a Incidentes de Seguridad Informática del Uruguay) de AGESIC.

En este contexto, la REDuy se convierte en el instrumento clave para la obtención de un Gobierno en Red. La infraestructura de conectividad de la misma posibilita que los organismos trabajen de forma integrada, bajo un marco técnico seguro para el intercambio de información; y además, permite racionalizar los recursos humanos y económicos"1

LaIlustración 2 Definición de PDImuestra a la Plataforma de Interoperabilidad como punto de conexión entre los distintos servicios del Estado, junto con los principales conceptos asociados a ella.

Plataforma de Interoperabilidad

Principales beneficios

Estandarización y reducción de costos

Cuando dos o más sistemas tienen la necesidad de interoperar, se debe realizar un consenso en lo que respecta a características como protocolos de comunicación, semántica de los mensajes, cómo va a ser la operativa diaria, cuál será el sistema de gobernanza de los servicios, entre otros.

Al momento de diseñar la Plataforma, estas características fueron acordadas y estandarizadas, de forma que los organismos que requieran publicar y/o consumir servicios a través de la misma no tengan que dedicar tiempos del proyecto en establecer estas definiciones. Esto lleva directamente a una reducción de costos del proyecto en lo que respecta a tiempos de definición y de implementación.

---

[1] Qué es la REDuy- Portal de AGESIC
http://www.agesic.gub.uy/innovaportal/v/3686/10/agesic/que-es.html

Estos beneficios son los que ofrece una arquitectura que está orientada a servicios. Esto implica que los servicios sean reutilizables, tengan una arquitectura flexible, y principalmente que favorece la Integración con sistemas legados. Independientemente de la tecnología que utilice un organismo en sus sistemas internos, puede interoperar con otros organismos a través de la PDI.

Principales características

A continuación se describen las principales características que ofrece la PDI:

- **Servicio de Control de Acceso**: se basa en la aplicación de políticas de AAA (autenticación, autorización y auditoría) de todas las transacciones que pasan por la Plataforma.

- **Servicio de Ruteo**: Cuando un cliente desea consumir un servicio publicado a través de la PDI, éste no conoce la dirección final de donde está alojado el servicio. Esto es posible gracias a un ruteo basado en contenido que realiza este servicio de ruteo. El mismo se basa en el estándar ws-addressing para mapear una dirección lógica enviada por el cliente contra el servicio final. Este servicio es fundamental para proteger la infraestructura de quienes publican servicios, manteniendo anónima su ubicación. Otro beneficio de este servicio, es que si existe algún problema en la infraestructura de quien publica un servicio, y éste tiene la necesidad de aplicar un mecanismo de contingencia que involucre levantar el servicio en otro servidor, desde la plataforma se pueden realizar las configuraciones necesarias para que estos cambios sean totalmente transparente para los clientes.

- **Servicio de novedades**: Implementado con un esquema Publish& Subscribe, permite que uno o más organismos puedan publicar novedades en un tópico determinado y que distintos organismos se suscriban a ese tópico y las consuman.

- **Servicio de administración y control de carga**: está orientado exclusivamente a proteger la infraestructura de los organismos que publican servicios. Por ejemplo si los organismos proveedores decidieran limitar la cantidad de invocaciones (por organismo o en total), se pueden realizar una serie de configuraciones en la Plataforma para establecer y hacer cumplir con estos límites.

- **Servicio Conector PGE**: es un software de caja negra destinado a facilitar la conexión contra la PDI. Contiene la lógica necesaria para conectarse a la Plataforma, en particular, autenticación y autorización.

- **Servicio Interfaces Web**: extiende las funcionalidades del conector. Además de facilitar la lógica ofrece una interfaz web para que un usuario de un organismo pueda invocar un servicio sin necesidad de desarrollar un código cliente.

- **Servicio de reportes estadísticos**: La aplicación de Reportes es un sistema orientado a brindar información estadística de aquellos servicios que son publicados y consumidos a través de la Plataforma de Interoperabilidad.
  A través de este sistema, los organismos podrán llevar a cabo un control detallado de cómo son utilizados los servicios que éstos publican, así como llevar adelante un control de consumo de los distintos servicios a los que éstos acceden. Por ejemplo, reportes de uso diario, semanal o mensual de un servicio.2

- **Servicio de monitoreo**: Está orientado a velar por la salud de los servicios que están publicados a través de la PDI. El objetivo es la detección de problemas de forma de solucionarlos de forma proactiva y no reactiva.

- **Servicio de metadatos**: Es un conjunto de esquemas definidos y que están disponibles para organismos que los requieran. Por ejemplo metadatos de empresas, direcciones o personas. El objetivo es reducir los tiempos de definición de la interoperabilidad semántica.

[2] Reportes sobre la Plataforma de Interoperabilidad - Portal de AGESIC http://www.agesic.gub.uy/innovaportal/v/3008/1/agesic/reportes_sobre_plataforma_de_interoperabilidad.html

Componentes de la PDI

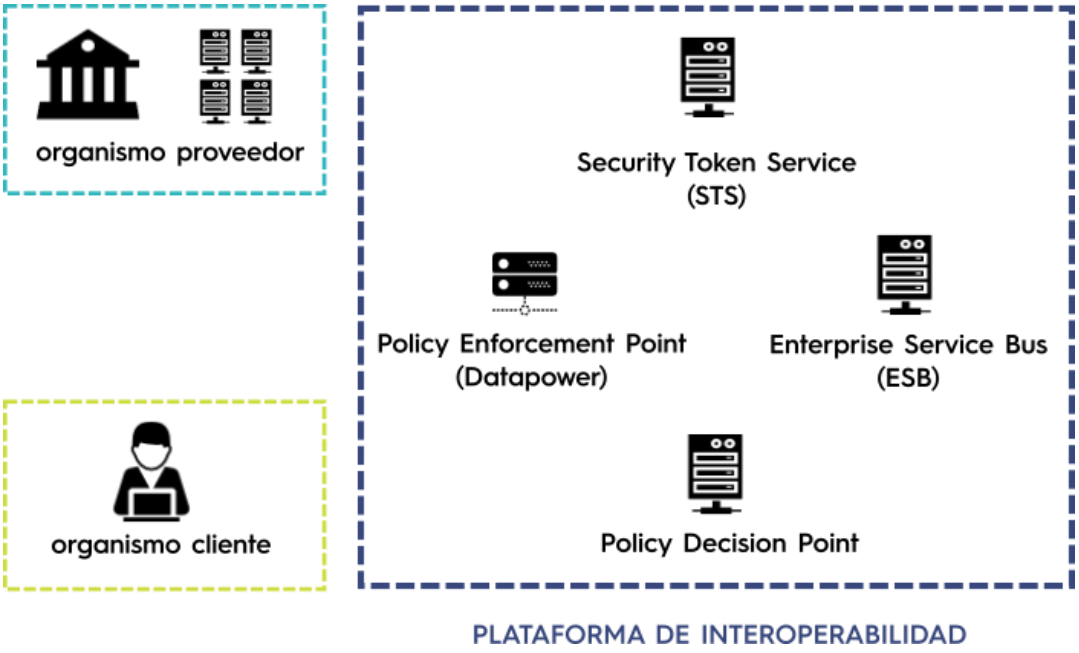

Ilustración 3 Componentes de la PDI

La Ilustración 3 Componentes de la PDIdescribe los principales componentes de la Plataforma. El organismo cliente es el que quiere consumir un webservice, el organismo proveedor es el que publica un servicio y la plataforma es el punto de contacto entre ambos.

El esquema de la plataforma está conformado por cuatro elementos:

- PolicyEnforcement Point: este es el punto de entrada a la Plataforma. Cuando un organismo cliente va a consumir un webservice a través de la PDI, este componente es el encargado de velar por el cumplimiento de las políticas de seguridad establecidas. Para esto, delega las políticas de autenticación y autorización a los componentes correspondientes. Una vez que se asegura que las políticas sean cumplidas, permite efectivamente realizar el consumo del servicio.

- Security TokenService (STS): Es un servicio encargado de emitir tokens SAML de seguridad de forma de autenticar la identidad de un organismo que intenta consumir un servicio a través de la PDI.

- PolicyDecision Point: Este componente tiene la responsabilidad de determinar si un organismo está autorizado o no para consumir un determinado servicio de la Plataforma.

- ESB: es el componente encargado del ruteo de los mensajes que pasan por la Plataforma. A su vez ofrece distintos servicios como ser el servicio de Novedades de la PDI.

Catálogo de servicios

El catálogo de servicios de AGESIC está disponible en el portal de AGESIC y contiene todos los servicios publicados por los organismos y disponibles para consumir.

En este catálogo se puede acceder a la descripción técnica y funcional de cada servicio, así como a los requerimientos necesarios para poder consumir un determinado servicio en la Plataforma. En algunos casos basta con enviar un correo al organismo proveedor del servicio pidiendo aprobación, y en otros casos es necesaria la firma de un convenio particular.

Para acceder al catálogo http://www.agesic.gub.uy/innovaportal/v/1602/9/agesic/catalogo-de-servicios.html

Consumo de servicios

Al momento de consumir un servicio debemos conocer cuáles son los mecanismos de seguridad que se aplican (servicio de seguridad) y cómo son los mecanismos de direccionamiento que se aplican (servicio de ruteo).

Como resultado del consumo de un webservice van a quedar registros de auditoría.

Servicios de seguridad

El servicio de seguridad se basa en la aplicación de políticas AAA (autorización, autenticación y auditoría). Además garantiza el no repudio de transacciones a través de distintos certificados (Certificados de infraestructura para establecer un canal SSL con autenticación mutua, y certificado de persona jurídica para firmar las transacciones). Por otra parte, la PDI previene los ataques de seguridad, en particular lo que refiere al top 10 definidos por la OWASP (Open Web Application Security Project)

Políticas AAA:

- **Autenticación** esun modelo basado en confianza, que se basa en la aplicación del estándar WS-Trust (estándar para la autenticación de servicios en ambientes federados) y SAML (define un formato de credenciales basado XML para poder representar identidades).

- **Autorización**: es un modelo basado RBAC. La plataforma no autoriza a usuarios, sino a roles dentro de una organización,es decir, áreas, sistemas propios, o la propia organización. La granularidad de permisos llega a nivel de método de un servicio. Es decir, se puede configurar la Plataforma para que permita que un organismo X tenga permisos únicamente de consumir un método en particular de un servicio.

- **Auditoría** Todas las transacciones llevadas a cabo por la Plataforma se encuentran auditadas. En particular, quedan registros asociados a quién consumió determinado servicio, cuándo lo hizo, y desde dónde.

Proceso de WS – Trust + SAML

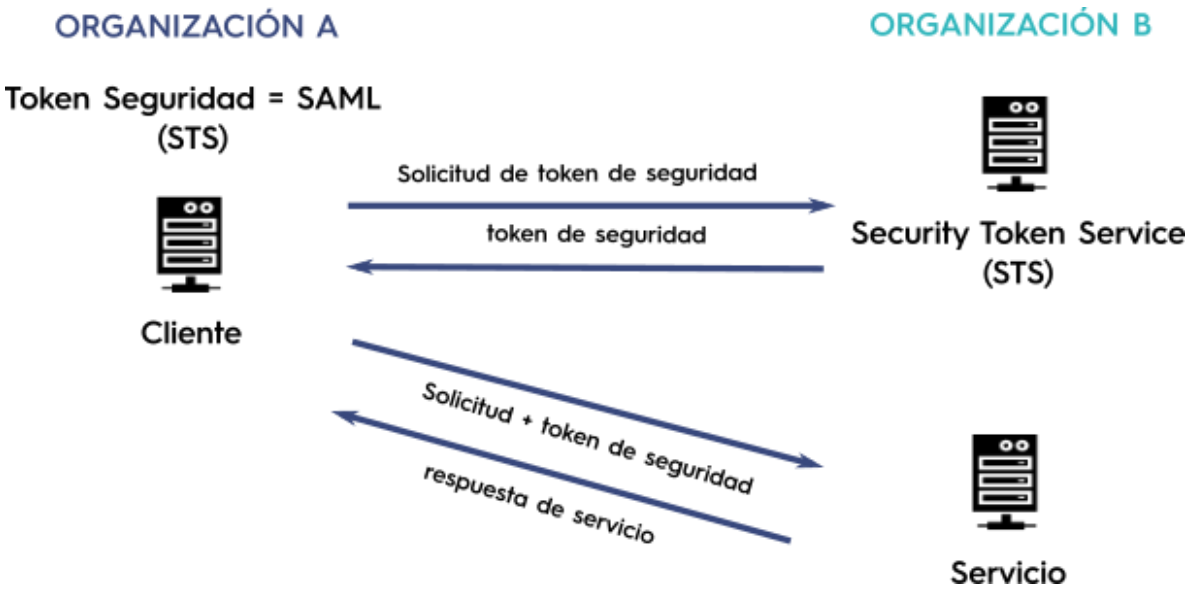

Ilustración 4 estándar WS – Trust y SAML

La figura anterior muestra cómo el estándar WS – Trust y SAML son utilizados en un esquema genérico.

Existen tres actores: Un servicio emisor de tokens de seguridad (STS), un servicio publicado que requiere autenticación de los clientes, y un Cliente que desea consumir el servicio publicado.

El cliente solicita un token de seguridad al STS para consumir un recurso específico. El STS verifica la firma del cliente, genera el token, lo firma, y lo devuelve al cliente. El cliente entonces envía el token firmado por el STS adjunto al mensaje. El servicio valida la firma del token y allí es que efectivamente valida que el Cliente es quien dice ser.

Para que el proceso funcione debe existir una relación de confianza entre el servicio y la entidad que emite los tokens. Cuando el pedido llega al servicio, éste valida que la firma corresponda al STS en quien confía.

Certificados

Para consumir un servicio a través de la PDI hay dos tipos de certificados que intervienen:

Certificados de infraestructura:

Utilizados para establecer la conexión segura con autenticación mutua, lo cual garantiza la seguridad en el canal de conexión de extremo a extremo.

Al momento de consumir un servicio a través de la Plataforma de Interoperabilidad, la misma presenta un certificado firmado por la entidad certificadora (CA) de AGESIC. Por ejemplo, en el caso de consumo de servicios en el ambiente de testing, el certificado que presenta la PDI es "testservicios.pge.red.uy".

Para que una aplicación cliente (Conector, aplicación Java, aplicación .Net) pueda comunicarse con la Plataforma, debe especificarse que el certificado que presenta la PDI es de confianza. Para esto puede o bien configurarse el certificado de la PDI como certificado de confianza (en testing "testservicios.pge.red.uy"), o se puede configurar el cliente para que confíe en cualquier certificado emitido por la CA de AGESIC. De elegir esta última opción, basta con configurar el certificado de la CA (en el caso de testing "HGTivoliCA") dentro del almacén de certificados de confianza. En algunas ocasiones esta opción no es recomendable ya que al configurar el certificado de la CA de AGESIC como certificado de confianza se está permitiendo que cualquier sistema que presente un certificado emitido esta CA se conecte con el servicio.

Una vez que se configura la aplicación cliente para confiar en el certificado que presenta la Plataforma, resta configurar el certificado que enviará el sistema a la PDI para establecer el canal seguro con autenticación mutua. Para ello, el cliente deberá presentar un certificado emitido por la CA de AGESIC. El trámite de obtención de este certificado se realiza a través de una solicitud a la mesa de servicios de AGESIC. Los mismos no tienen costo y su período de validez es de un año.

Certificados de persona jurídica:

Son utilizados para firmar las transacciones, dándole un marco legal a las mismas.

A diferencia de los certificados de Infraestructura, estos certificados son utilizados para firmar las transacciones que suceden a través de la Plataforma. Para ello, el sistema cliente utiliza el certificado de persona jurídica perteneciente al organismo con el fin de firmar la solicitud de token de seguridad. Dado que este certificado pertenece a la institución, se garantiza la identidad de la misma y el no repudio de las transacciones. Esto brinda un carácter legal a los intercambios de información a través de la PDI. Vale destacar que la Plataforma no autentica a personas, sino a Organismos o Instituciones en el entendido de

que son estas quienes son responsables por la transacción. Por esto es que se usan certificados de persona jurídica y no de persona física.

Estos certificados pueden ser emitidos por cualquier distribuidor autorizado de firma electrónica avanzada, por ejemplo el Correo Uruguayo, y cada cliente debe hacer las gestiones necesarias con la institución para obtenerlos.

Nota

Existe un convenio entre AGESIC y Correo Uruguayo a través del cual la primera vez que el organismo hace la solicitud del certificado los gastos corren por cuenta de AGESIC. A medida que se que se realicen eventuales actualizaciones, los gastos correrán por cuenta del organismo. Por más información sobre los certificados de Correo Uruguayo: www.correo.com.uy

Servicio de ruteo

El servicio de Ruteo está orientado a desacoplar el cliente del servidor y por lo tanto protege la infraestructura de aquellos organismos que publican servicios a través de la Plataforma. Este servicio permite que los clientes de la PDI puedan consumir un servicio sin conocer la dirección física de donde el servicio está efectivamente publicado.

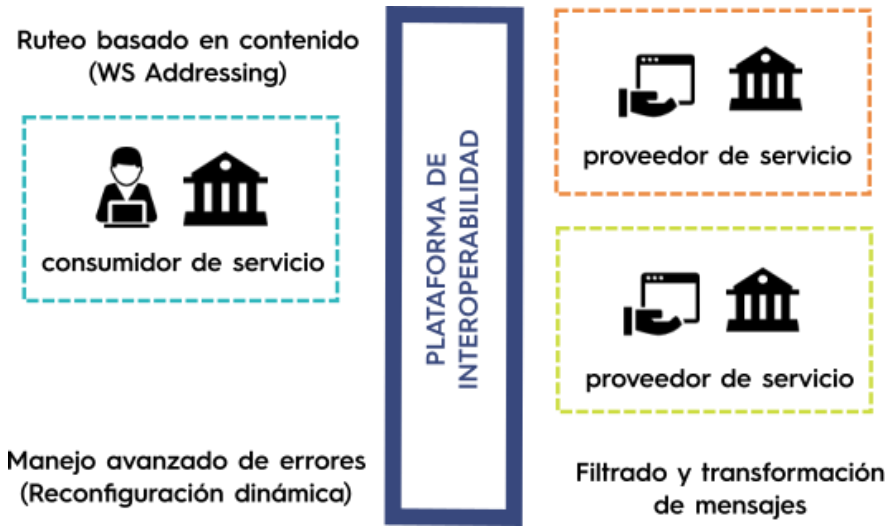

Ilustración 5 Ruteo de servicios

Usando un ruteo basado en contenido, a través del estándar WS-Adressing, el cliente indica en el cabezal del mensaje Soap cuál es el servicio que desea consumir. Este servicio está representado por una URL Lógica, la cual es capturada por el servicio de ruteo y mapeada con la dirección física en la que efectivamente el servicio está publicado. Luego de este Mapeo, el ruteo redirige el pedido al proveedor final.

Otro beneficio de este servicio es que en caso de existir algún inconveniente en la infraestructura del organismo proveedor, y algún mecanismo de contingencia debe ser puesto en funcionamiento, el servicio de Ruteo puede reconfigurar la dirección física final del web service de forma que el cambio sea totalmente transparente para los clientes del mismo. Esto reduce posibles impactos en el negocio de los clientes.

Por otra parte, el servicio de Ruteo permite, en casos excepcionales, realizar transformaciones sobre los mensajes que por allí pasan. Estas transformaciones se pueden realizar en casos en que es realmente necesario para el negocio y ni el proveedor del servicio ni los tienen la posibilidad de realizarlas.

Escenario de Consumo de servicios en PDI

El siguiente diagrama muestra las principales interacciones entre los componentes de la PDI que se dan al momento de consumir un web service a través de la misma.

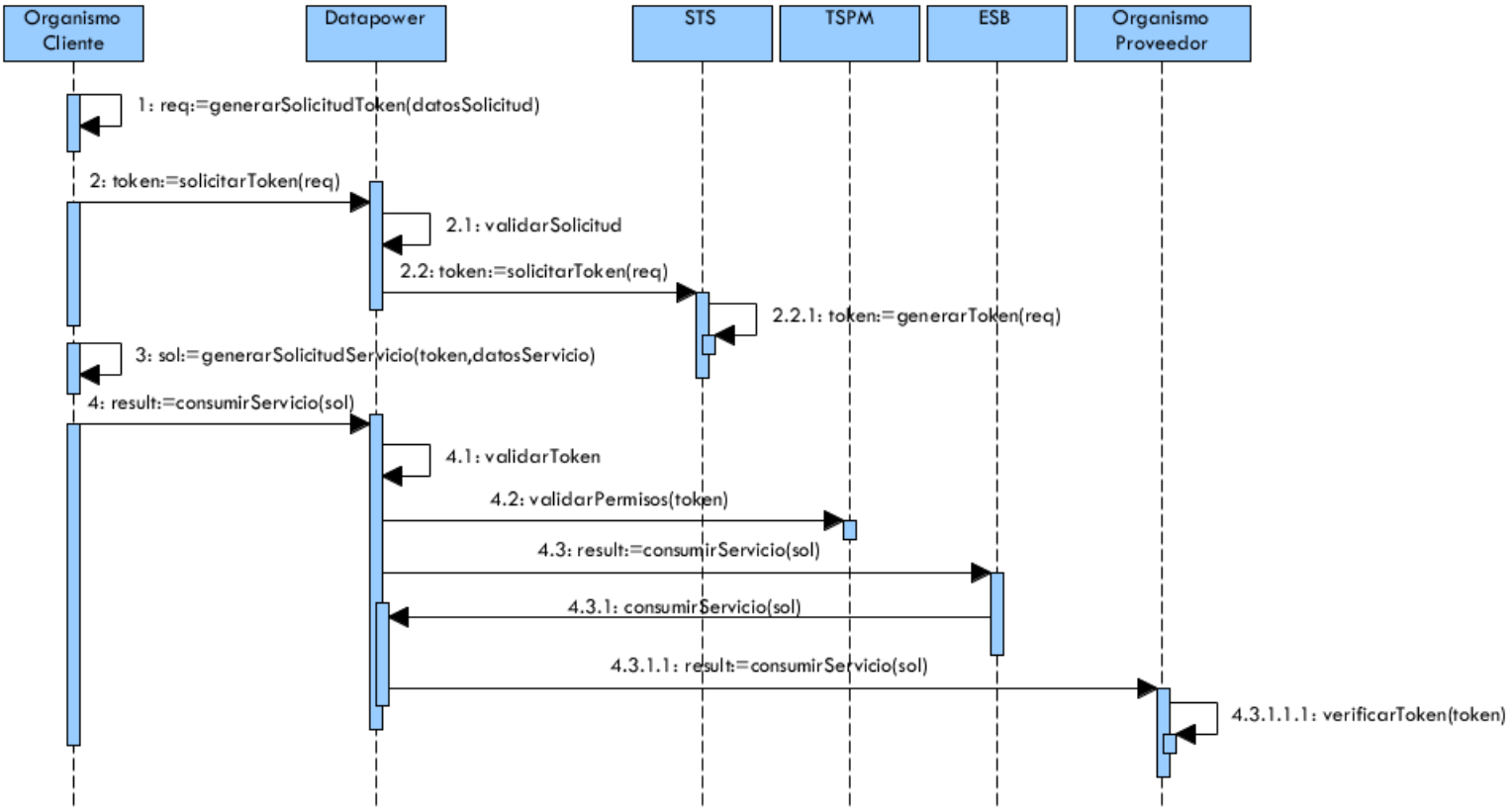

Ilustración 6 Interacciones entre los componentes de la PDI

Descripción del escenario

Como precondición, debe existir una relación de confianza entre el organismo proveedor de un servicio y el STS de la Plataforma.

1. El organismo cliente arma un mensaje de solicitud de tokenSAML que va a incluir como parte del mismo la siguiente información:

    - Rol del organismo

- Nombre de usuario (opcional)
- Servicio que desea consumir
- Firma del organismo(con certificado de persona jurídica).

2. El organismo se comunica con Datapower(punto de entrada a la Plataforma) para realizar la solicitud de token.

   2.1 Datapower verifica la firma del token SAML.

   2.1. Una vez que la valida redirige el pedido a la entidad emisora de token.

   2.2. La entidad verifica los datos y emite un nuevo token SAML. Este token contendrá la información original que fue enviada por el cliente más la firma de la entidad.

3. Para consumir el webservice, el cliente construye un mensaje que contendrá los datos del negocio (parámetros del servicio), los datos de ruteo (dirección lógica y método que desea consumir), y adjuntará el token de seguridad emitido por el STS, que avala que ese cliente está autenticado y es quién dice ser.

4. El cliente envía el mensaje construido en el paso anterior a la Plataforma, solicitando a la PDI consumir este servicio.

   4.1. La PDI verifica que el token sea válido y no haya expirado.

   4.2. La PDI después delega al PolicyDecision Point (TSPM)la responsabilidad de comprobar si el contenido dentro del token se encuentra habilitadopara consumir ese servicio.

   4.3. En caso de estar habilitado para consumir el servicio, el datapowerdelega al ESB la responsabilidad de redireccionar el pedido a la dirección física correspondiente.

      4.3.1. El ESB (particularmente el servicio de Ruteo) redirecciona la solicitud a través de DataPower.

      4.3.1.1. DataPower establece la comunicación con el proveedor del servicio con el fin de hacer la soliciltud final.

      4.3.1.1.1. El proveedor del servicio, opcionalmente, valida que el token adjunto en la solicitud sea proveniente de la entidad emisora de tokens en la cual confía. En ese caso, procesa la solicitud y devuelve la respuesta correspondiente de cara al cliente original.

Modalidad para consumir un servicio

Cuando un organismo desea consumir un servicio web expuesto en la Plataforma de Gobierno Electrónico (PGE), hay varios aspectos que deben ser considerados. Entre ellos, se destacan el marco legal y técnico, intercambio seguro de información, y la participación en una arquitectura orientada a servicios (SOA). Estos aspectos requieren de cierto grado de madurez tecnológica, que muchas veces no se tiene en los organismos.

Para facilitar el proceso de invocación AGESIC ha desarrollado distintas alternativas como ser bibliotecas Java y .Net, y en particular, un aplicativo que hace transparente la complejidad de invocar servicios en la PGE. Este aplicativo es denominado Conector PGE.

Procedimiento para consumir un servicio en la PDI

1. Enviar un correo a Mesa de Servicios soporte@agesic.gub.uy adjuntando el formulario de solicitud de consumo de servicio.

2. Solicitar autorización al organismo proveedor. Para esto es suficiente con reenviar un e-mail del organismo confirmando la autorización, con excepción de los siguientes organismos:

2.1 Si es un servicio provisto por la DNIC se deberá solicitar una solicitud formal

2.2 Si es un servicio provisto por la DGI es suficiente con notificar vía mail el consumo del servicio a la Secretaría de Informática (secinfo@dgi.gub.uy) copiando a soporte@agesic.gub.uy en el correo.

Paralelamente, se podrá ir avanzando en:

A) Configuración de seguridad

A.1) Emitir un certificado para SSL

Enviar a Mesa de Servicios el certificado PKCS10. En nuestro servidor SFTP podrán encontrar tutoriales (NET/JAVA) que los guiarán paso a paso para realizar esta tarea.

host: sftp://sftp.agesic.gub.uy/uploads
Usuario: Plataforma.
Password: P1ataf0rma2014.

A.2) Emitir un certificado Pesona Jurídica (organismo)

Otro certificado necesario para consumir el servicio es el certificado de Organismo emitido por el Correo Uruguayo que se utiliza para firmar la petición a la Plataforma para su consumo. Este certificado es el de Persona Jurídica, por más información e instrucciones dirigirse al sitio del Correo Uruguayo (http://www.correo.com.uy/index.asp?g=1,16&seccion=383).

B) Desarrollo del cliente

Si es su primera experiencia en el consumo de Servicios de Plataforma, se recomienda desarrollar un cliente de prueba que consuma nuestro servicio de testing. En nuestro servidor FTP podrán encontrar tutoriales (NET/JAVA) que los guiarán paso a paso en esta tarea.

Una vez culminada esta actividad, se está en condiciones de desarrollar el cliente para el servicio solicitado. Para ello se adjunta la ficha del Servicio y el WSDL correspondiente.

Por otro lado, el equipo de Tecnología se comunicará con Uds. para conocer el contexto de uso de esta solicitud así como los plazos y necesidades de su proyecto.

Ante cualquier duda o consulta pueden contactarse con Mesa de Servicios a soporte@agesic.gub.uy o al 29010065

Conector PGE

El Conector PGE es un software de caja negra cuyo objetivo es facilitar el consumo de web services a través de la Plataforma de Interoperabilidad.

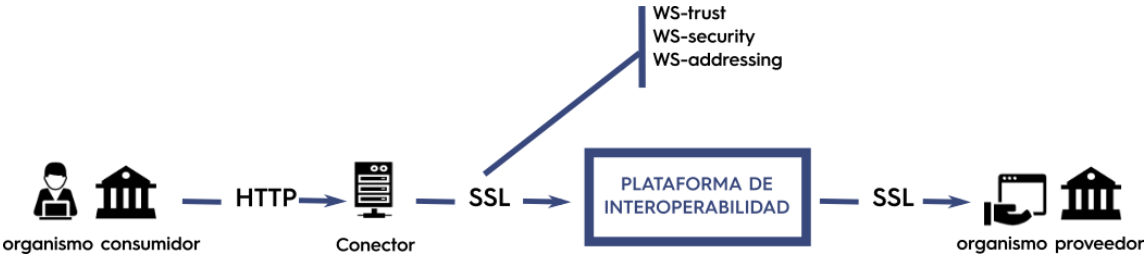

Ilustración 7 Consumo a través del Conector

El Conector se ejecuta dentro de la infraestructura del cliente (el organismo que desea consumir servicios a través de la PGE instala el Conector en su red privada) y básicamente su propósito es actuar como servidor proxy para la invocación a servicios en la PGE: para cada servicio expuesto en la PGE y que se desee consumir se podrá configurar un servicio virtual en el Conector, llamado “servicio proxy” que represente al servicio real, el cual ofrece exactamente las mismas operaciones pero sin restricciones de seguridad, siendo el Conector el encargado de aplicar dichas restricciones para luego invocar el servicio final.

De esta manera, los clientes finales invocarán al servicio virtual en el Conector, éste tomará los pedidos, enriquecerá el mensaje con lo requerido por la PGE (información de seguridad, autenticación y direccionamiento) e invocará al servicio en la PGE. Una vez obtenido el resultado, el Conector lo retornará al cliente como si fuese el servicio final. Un diagrama de la arquitectura general se ilustra en la siguiente figura:

Reportes[3]

Información General

La aplicación de Reportes es un sistema orientado a brindar información estadística de aquellos servicios que son publicados o consumidos a través de la Plataforma de Interoperabilidad.
A través de este sistema, los organismos podrán llevar a cabo un control detallado de cómo son utilizados los servicios que éstos publican, así como llevar adelante un control de consumo de los distintos servicios a los que éstos acceden. Por ejemplo, reportes de uso diario, semanal o mensual de un servicio.

Descripción funcional

Entre las principales características se encuentran:

Invocaciones de servicio

Permite visualizar para un período de tiempo determinado, la cantidad de invocaciones a cada servicio publicado por el organismo en ese período de tiempo.

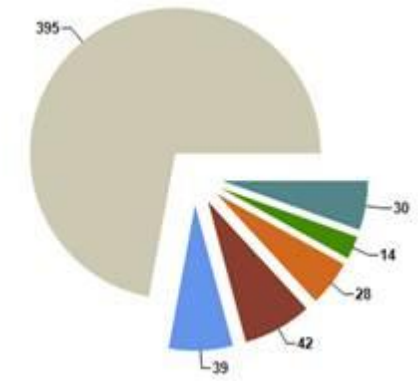

Ilustración 8 Reporte Invocaciones de Servicio

Evolución de consumo por mes

Permite visualizar cómo es la evolución de consumo de un servicio publicado por un organismo en un período de tiempo. En el mismo, se muestra la cantidad de consumos que realiza cada organismo día a día.

[3] Reportes sobre la Plataforma de Interoperabilidad - Portal de AGESIC http://www.agesic.gub.uy/innovaportal/v/3008/1/agesic/reportes_sobre_plataforma_de_interoperabilidad.html

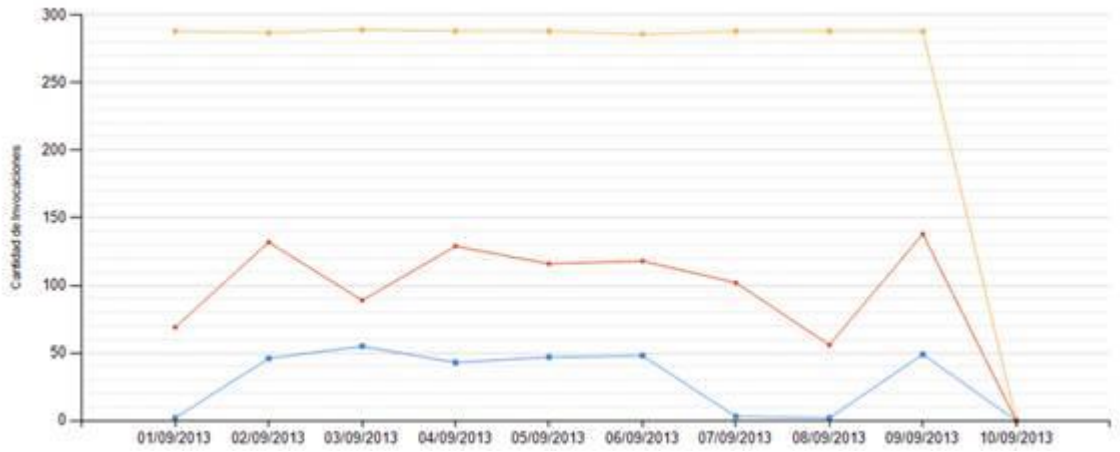

Ilustración 9 Reporte Evolución de consumo en meses

Evolución de consumo por hora

Permite visualizar cómo es la evolución de consumo de un servicio publicado por un organismo en un día determinado. En el gráfico se muestra la cantidad de consumos que realiza cada organismo hora a hora.

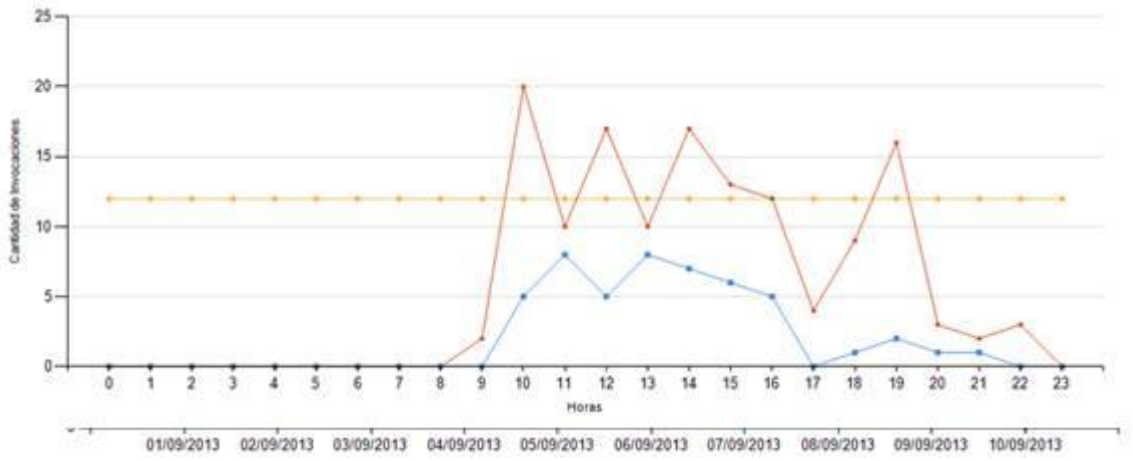

Ilustración 10 Reporte Evolución de consumo por hora

Invocaciones por Organismo

Este gráfico muestra, para un período de tiempo determinado, la cantidad de invocaciones realizadas a un servicio determinado discriminando por organismos. A su vez, muestra la cantidad de invocaciones con error.

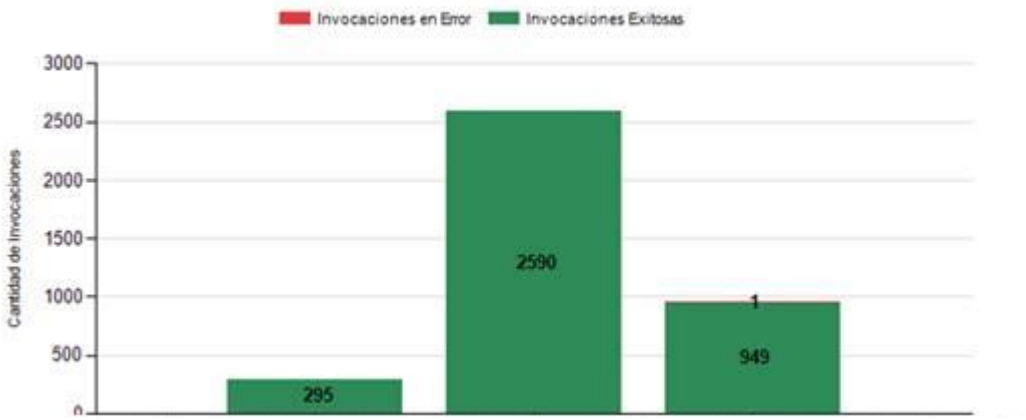

Ilustración 11 Reporte invocaciones por organismo

Detalle de Consumo

Este reporte permite visualizar la información de consumo de un servicio de forma detallada indicando la operación consumida, el organismo consumidor, fecha y hora de la invocación, resultado (éxito/error), tiempo de respuesta del servicio, y mensaje de error en caso de haber existido algún problema. A su vez, se permite la posibilidad de exportar los resultados en distintos formatos (csv, Excel, pdf). Esto da la posibilidad de que cada organismo pueda generar sus propios reportes a partir de la información brindada.

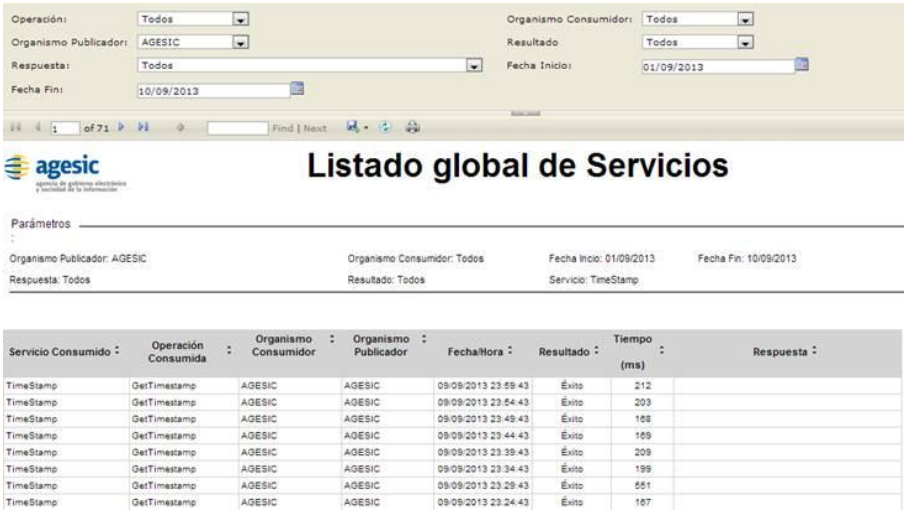

Ilustración 12 Reporte Detalle de consumo

Conclusiones

La Plataforma de Interoperabilidad es un componente fundamental para facilitar la interoperabilidad entre los sistemas de los distintos organismos del Estado, brindando un marco legal y técnico a todas las transacciones que por allí pasan.

Por otro lado, la PDI brinda un conjunto de beneficios y características que son ofrecidas tanto para aquellos organismos que desean publicar un servicio como para aquellos organismos que desean consumir servicios a través de la misma.

En el presente documento, se mostraron los principales conceptos asociados a la PDI, haciendo énfasis en los servicios, características de seguridad y beneficios, así como sus principales características de seguridad.

Por otro lado, se presentó un escenario de ejemplo de consumo de servicios, el cual puede ser implementado siguiendo los distintos tutoriales que acompañan el curso. Estos tutoriales incluyen consumo de servicios usando bibliotecas Java, bibliotecas .Net, y consumo de servicios utilizando el Conector PGE.