Conector PGE

Documento de Arquitectura

Área de Tecnología

División Arquitectura

**Historial de Revisiones**

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Versión | Cambios | Autor |
| 10/01/2018 | 1.0 | Creación del documento | Equipo Pyxis |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Tabla de contenido

[Tabla de contenido 3](#_Toc503374289)

[1 Introducción 4](#_Toc503374290)

[1.1 Objetivo del documento 4](#_Toc503374291)

[1.2 Público objetivo 4](#_Toc503374292)

[1.3 Actualización 4](#_Toc503374293)

[1.4 Definiciones, acrónimos y abreviaturas 4](#_Toc503374294)

[2 Resumen ejecutivo 5](#_Toc503374295)

[3 Arquitectura 6](#_Toc503374296)

[3.1 Vista de Casos de Uso 6](#_Toc503374297)

[3.2 Vista de componentes lógicos 7](#_Toc503374298)

[3.3 Vista de componentes físicos 8](#_Toc503374299)

[3.4 Vista de procesos 10](#_Toc503374300)

[3.5 Vista de despliegue 13](#_Toc503374301)

[3.6 Vista de estándares 14](#_Toc503374302)

# Introducción

## Objetivo del documento

El objetivo del presente documento es documentar la arquitectura del Conector PGE. Esta documentación está dada por la definición de un conjunto de vistas complementarias que en su conjunto definen la arquitectura del sistema.

## Público objetivo

Este documento está dirigido al equipo de arquitectura de AGESIC, arquitectos y desarrolladores del Conector PGE.

## Actualización

Este documento se actualizará cada vez que se analice/diseñe un requerimiento el cual implique cambios en la arquitectura del sistema. Por cambios en la arquitectura entendemos, cambios en los componentes, su forma de comunicación con otro componente o interfaz.

## Definiciones, acrónimos y abreviaturas

|  |  |
| --- | --- |
| Término | Descripción |
| AGESIC | Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. |
| PDI | Plataforma de Interoperabilidad de AGESIC |
| STS | Security Token Service |

# Resumen ejecutivo

Para facilitar el proceso de invocación AGESIC ha desarrollado un aplicativo que hace transparente la complejidad de invocar servicios en la PGE. Este aplicativo es denominado Conector PGE simplemente Conector.

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 no siempre está presente en los organismos del Estado.

El Conector se ejecuta dentro de la infraestructura del cliente, es decir, el organismo que desea consumir servicios a través de la PGE instala el "Conector" en su red privada. Su propósito es actuar como servidor proxy para la invocación a servicios en la PGE: para cada servicio expuesto, 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.

La Figura 1 ilustra estos conceptos.

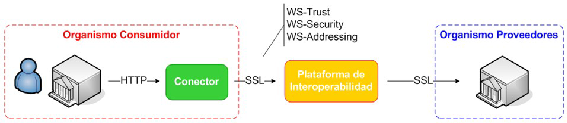


Figura - Visión general del Conector PGE

# Arquitectura

La Arquitectura del Conector está descrita según un conjunto de vistas independientes pero complementarias que combinadas permiten mostrar una visión completa. Las vistas consideradas en este documento son:

* Vista de casos de uso: describe brevemente los casos de uso más relevantes para la arquitectura.
* Vista lógica: describe los componentes lógicos de la arquitectura.
* Vista de procesos: describe brevemente los procesos más relevantes para la arquitectura.
* Vista de despliegue: describe como estarán distribuidos los diferentes componentes de la arquitectura en la infraestructura física del Ministerio y si estos se encuentran o no en alta disponibilidad.
* Vista de estándares: describe los estándares más relevantes que son utilizados por la arquitectura.

## Vista de Casos de Uso

En esta sección se presentan los diagramas casos de uso relevantes para la arquitectura y que tienen un impacto directo en la arquitectura del Conector (p. ej: definición de componentes, interfaces o protocolos de comunicación).

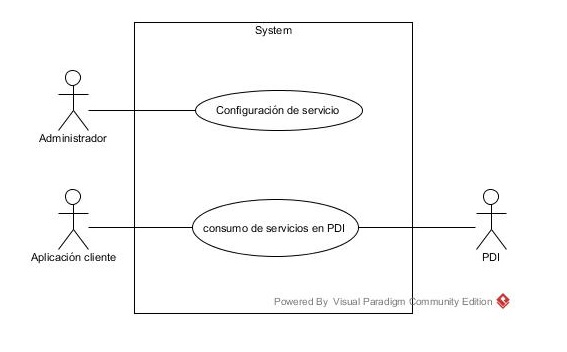


Figura – Vista de casos de uso

### Configuración de servicio

Este caso de uso implica que un administrador del organismo encargado del Conector, crea una configuración de un servicio en el Conector para luego consumir un servicio de la PDI. Desde la consola de administración web, el administrador ingresa la información necesaria. Esta información será utilizada luego en el caso de uso Consumo de servicios en PDI.

### Consumo de servicios en PDI

Este caso de uso implica que una aplicación cliente de un organismo consume un servicio de la PDI En este escenario, la aplicación cliente envía un mensaje SOAP a un servicio en el Conector, el cual se encarga de agregarle información de seguridad y ruteo al mensaje, según la configuración definida del servicio PDI del Conector. Con esta información el Conector solicita un token de seguridad a la PDI y luego, con este token, reenvía el pedido al servicio de la PDI. La respuesta recibida, se envía a la aplicación cliente.

## Vista de componentes lógicos

Esta vista describe los componentes lógicos del conector a nivel conceptual, identificando sus responsabilidades y dependencias entre ellos. La Figura 3 los presenta gráficamente.

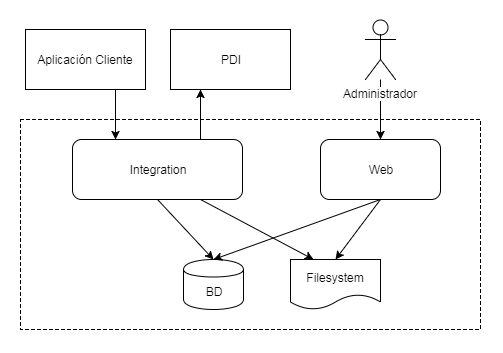


Figura - Vista de componentes lógicos

El conector PGE está compuesto por dos grandes componentes: 1) componente web y 2) componente de integración. El componente web tiene como propósito proveer una interfaz de administración web, donde el administrador podrá configurar los servicios de la PDI a consumir, así como también uso de keystores, trustores, exportar e importar configuraciones. Por otro lado, el componente de integración permite a las aplicaciones cliente de un organismo consumir un servicio de la PDI de forma simplificada, sin requerir los estándares de la PDI (p.ej: WS-Trust, WS-Addressing). Ambos componentes se apoyan en una base de datos y el filesystem para almacenar la configuración, donde la información relacional se almacena en base de datos y la archivos en el filesystem (p.ej: wsdl, keystores y truststores).

## Vista de componentes físicos

Un componente físico es un artefacto de implementación (jar, war, etc) encargado de materializar uno o más componentes lógicos descritos en la sección 3.2. La Figura 4 describe gráficamente los componentes físicos del Conector.

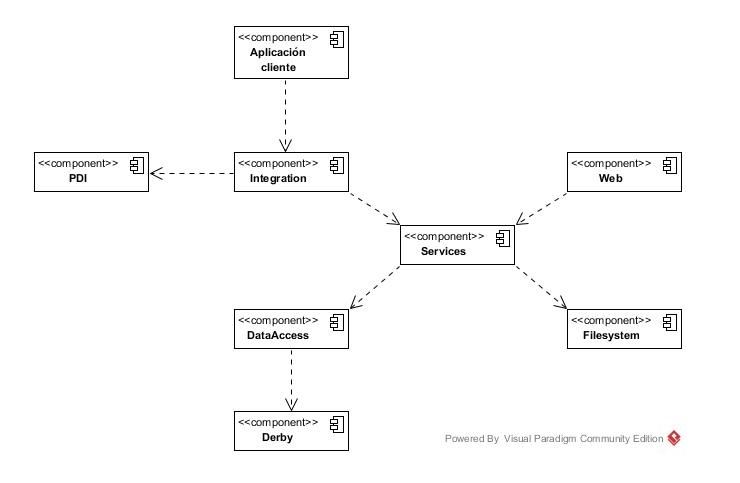


Figura - Vista de componentes físicos

**Componente DataAccess**

Este componente tiene como propósito proveer una interfaz para acceder a los datos de configuración del Conector y abstraer el mecanismo de persistencia utilizado. Este componente se comunica con una base de datos Derby para almacenar los datos.

**Componente Filesystem**

Este componente refleja el filesystem donde está alojado el conector. En este filesystem se alojan archivos de configuración como ser wsdl, keystore y truststores.

**Componente Services**

Este componente es el encargado de ofrecer un conjunto de interfaces de negocio para realizar la gestión de la configuración del Conector. En él se encuentra todas las reglas de negocio de la aplicación y provee un conjunto de interfaces para el alta, baja, modificación y consulta de configuraciones. Este componente se comunica con los componentes DataAccess y Filesystem para consultar o guardar información de configuración.

**Componente Integration**

Este componente es el encargado proveer la conectividad entre las aplicaciones cliente de un organismo y los servicios de la PDI. Provee una interfaz http para que las aplicaciones cliente puedan enviar un mensaje SOAP con destino a un servicio de la PDI. Estos mensajes son transformados según la configuración definida en el Conector para ese servicio.

Este componente se comunica con el componente Services para consultar la configuración de un servicio en el conector y con la PDI para solicitar un token y luego consultar el servicio publicado en ella.

**Componente Web**

Este componente tiene como propósito proveer una interfaz Web de administración del Conector, donde un usuario administrador pueda dar de alta, modificar, borrar y consultar la configuración de un servicio en el Conector. Este componente se comunica con el componente Services para poder llevar a cabo sus funcionalidades.

**Trazabilidad con la vista lógica**

En la vista lógica presentada en la sección 3.2 se presentaron los componentes lógicos de la arquitectura, mientras que, en esta vista, se presentan sus componentes físicos. En la Tabla 1 se presenta qué componentes físicos implementan cada uno de los componentes lógicos. Aquellos componentes que participan. Existen algunos componentes físicos que participan en más de un componente lógico.

|  |  |
| --- | --- |
| Componente lógico | Componente físico |
| Integration | Integration  Services  DataAccess  Filesystem |
| Web | Web  Services  DataAccess  Filesystem |

Tabla - Trazabilidad entre componentes lógicos y componentes físicos

## Vista de procesos

En esta vista se describen con más detalle los casos de uso descritos en la sección 3.1, utilizando para ello, los componentes descritos en la vista de componentes físicos. Esta vista se representa mediante diagramas de secuencia de sistema utilizando componentes físicos como unidad de trabajo.

### Configuración de servicio

Este escenario consiste en que un administrador salva la configuración para consumir un un servicio de la PDI. Los datos relacionales son almacenados en la base de datos Derby, mientras que los archivos son almacenados en el filesystem.

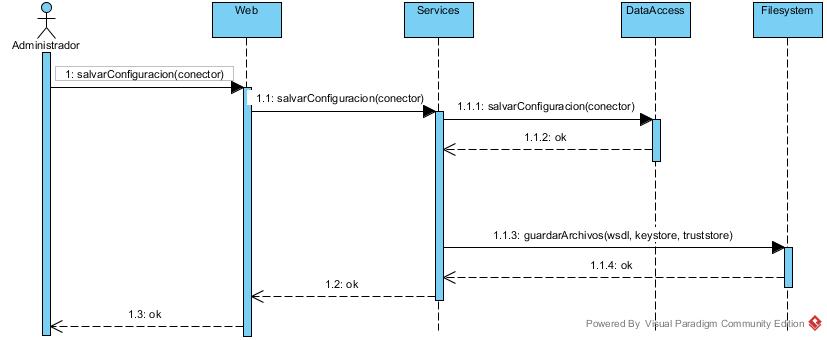


Figura - Diagrama de secuencia para configuración de servicios

### Consumo de servicios en PDI

El consumo de servicios de la PDI se compone de dos escenarios: 1) Consumo de un servicio básico (Figura 6) y 2) Consumo de un servicio utilizando MTOM (Figura 7).

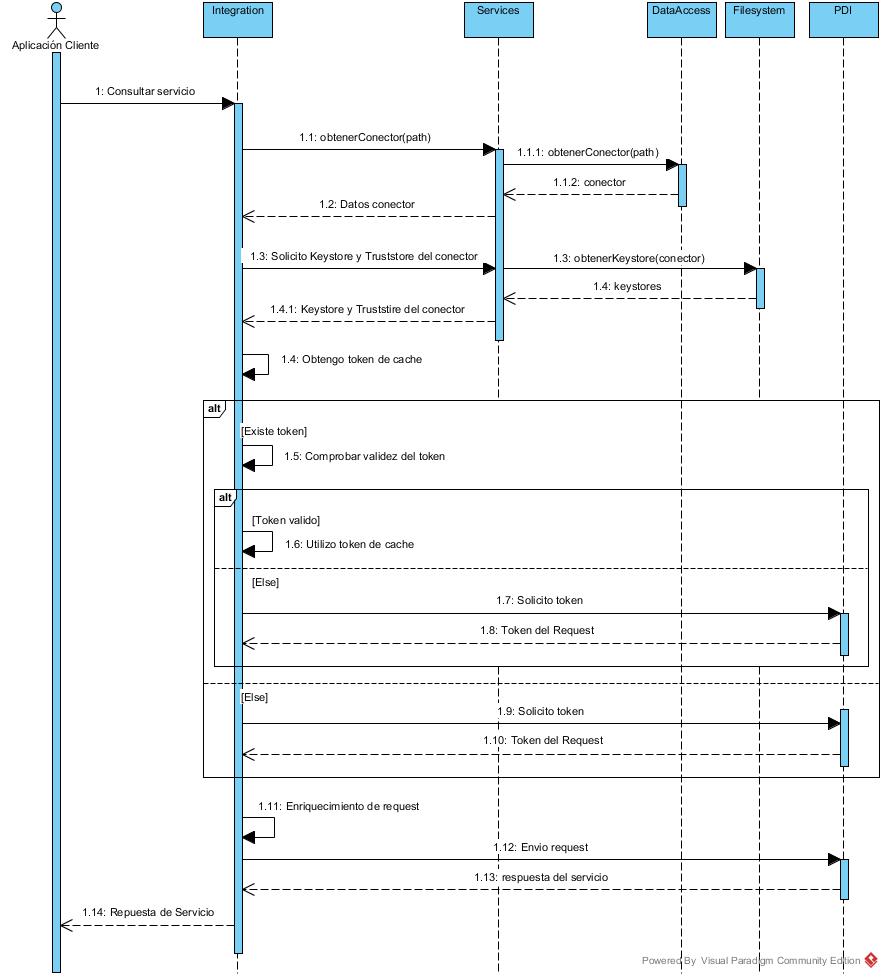


Figura - Diagrama de secuencia para consumo de servicio básico de la PDI

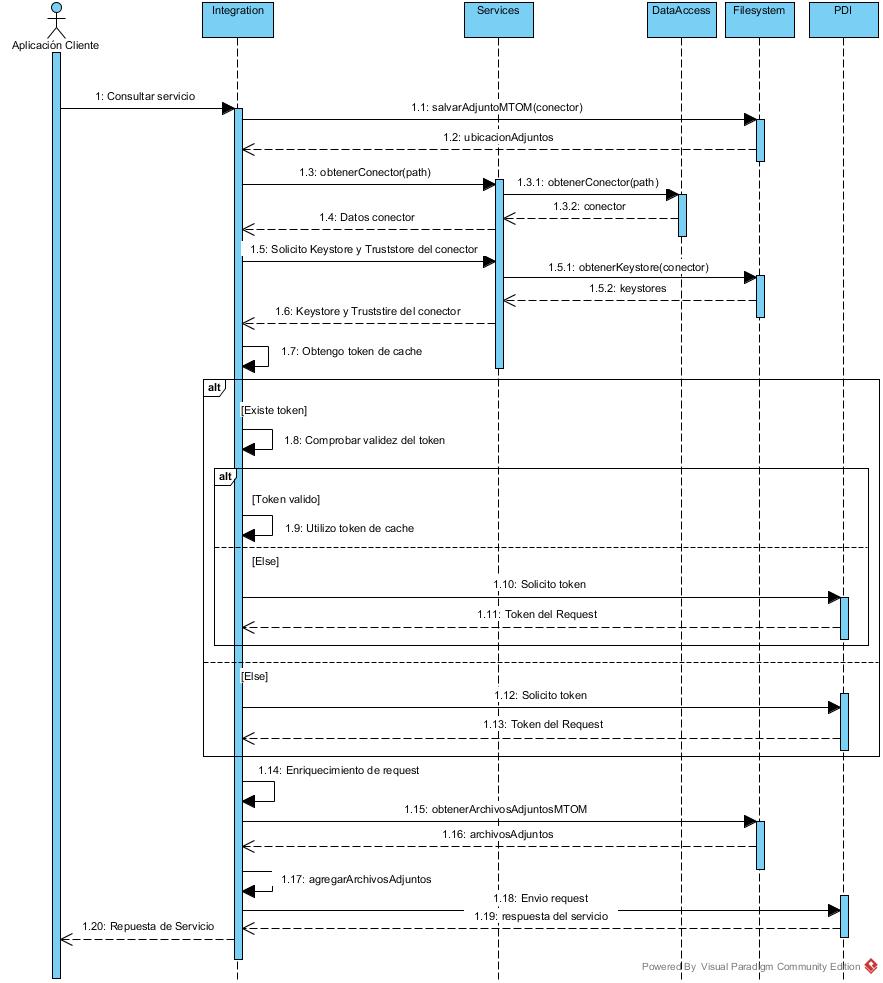


Figura - Diagrama de secuencia para consumo de servicio PDI con MTOM

## Vista de despliegue

La Figura 8 presenta gráficamente la vista de despliegue de la arquitectura. Esta vista describe cómo se despliegan los componentes físicos de la sección 3.3 sobre la infraestructura del organismo. Los nodos coloreados en blanco corresponden a la infraestructura del organismo, mientras que los nodos coloreados en gris corresponden a infraestructura de terceros (p.ej: AGESIC).

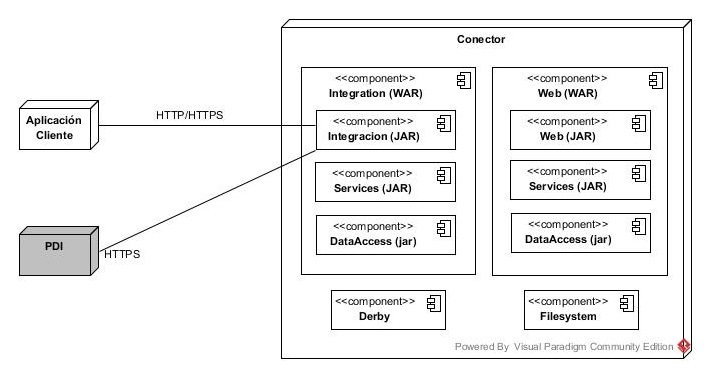


Figura - Diagrama de despliegue

**Nodo Conector**

Este nodo contiene todos los artefactos del Conector: 1) Integration, 2) Web, 3) Derby y 4) Filesystem. Los artefactos Integration y Web son dos aplicaciones Web desarrolladas en Java (WAR) que se hostean en el servidor Web (Tomcat o Wildfly). El artefacto Derby se corresponde con la base de datos Derby. Por último, el Filesystem representa el sistema de archivos del servidor donde se aloja el Conector.

**Nodo Aplicación Cliente**

Este nodo representa una aplicación cliente dentro del organismo.

**Nodo PDI**

Este nodo representa la Plataforma de Interoperabilidad de AGESIC.

## Vista de estándares

En esta vista se presenta los estándares más importantes utilizados por el Conector en su arquitectura. La Tabla 2 lista cada uno de ellos y describe su uso.

|  |  |  |
| --- | --- | --- |
| Estándar | Versión | Descripción de uso |
| WS-Trust | Febrero 2005 | Se utiliza como protocolo de comunicación para solicitar un token de seguridad al STS de la PDI. |
| WS-Security | 1.1 | Se utiliza como protocolo de comunicación para consumir un servicio de la PDI y adjuntar el token de seguridad emitido por el STS |
| SAML | 1.1 | Se utiliza como formato de tokens de seguridad para autenticarse contra la STS de la PDI y en la autenticación de servicios de la PDI |
| WS-Addressing | 1.0 | Se utiliza para identificar lógicamente a qué servicio va destinado el mensaje. |
| TLS | No aplica | Se utiliza para mantener la confidencialidad e integridad en la comunicación entre la aplicación cliente del organismo y el Conector y entre el Conector y la PDI |

Tabla 2 - Estandares utilizados por el Conector