Capítulo V

Alta y Consumo de Servicios

Introducción

Este capítulo describe, a nivel técnico, los requerimientos y pasos necesarios para que un organismo provea y consuma servicios en la PGE.

Alta de un Servicio en la PGE

Prerrequisitos

Para que un organismo pueda proveer un servicio en la PGE es necesario que esté conectado a la REDuy. Si no se cuenta con conexión a la REDuy consultar la sección "**¡Error! No se encuentra el origen de la referencia.**".

Implementación, Despliegue y Ejecución del Servicio

Los servicios que proveen los organismos se despliegan y ejecutan principalmente en sus servidores. Si se quiere alojar un servicio en la PGE consultar la sección "Ejecución de un Servicio en la PGE".

La implementación de los servicios puede realizarse utilizando diferentes tecnologías y plataformas como Java EE, .NET, PHP u otras. Cualquiera sea la tecnología que se utilice, los servicios a publicarse en la PGE deben cumplir con los siguientes requerimientos:

1. deben poder ser invocados mediante el envío, vía HTTPS, de mensajes que se ajusten al estándar SOAP (versión 1.1)

2. deben describirse utilizando el estándar WSDL (versión 1.1)

3. deben ajustarse a los lineamientos especificados en el Basic Profile (versión 1.1) [1] y Basic Security Profile (versión 1.0) [2] de la organización WS-I

4. el WSDL que describe al servicio debe incluir documentación general del servicio y documentación detallada de sus operaciones y parámetros de entrada y salida

Es importante mencionar que los servicios pueden implementarse completamente desde cero o apoyarse en Sistemas Legados existentes, permitiendo así su re-utilización y aprovechamiento.

Completar y Enviar Formulario "Alta de un Servicio"

Para exponer un servicio en la PGE, los organismos deben completar y enviar a AGESIC el "**¡Error! No se encuentra el origen de la referencia.**" que se encuentra en el Apéndice 2. En este formulario se debe especificar información general, ubicación, descripción, e información técnica y de seguridad del servicio. El formulario debe ser enviado por correo electrónico a la dirección soporte@agesic.gub.uy, especificando en el asunto del correo "[Alta de un Servicio en la PGE] *Nombre del Organismo Proveedor*".

Una vez aprobada la solicitud de alta de servicio, el equipo de soporte de AGESIC configura los *firewalls* de REDuy para habilitar el tráfico de red desde la PGE hacia el servicio, como se explica en la sección "**¡Error! No se encuentra el origen de la referencia.**".

En las próximas sub-secciones se describe la información que se debe incluir en el "**¡Error! No se encuentra el origen de la referencia.**".

Información General de la Solicitud

En primer lugar, el organismo debe brindarle a AGESIC información general sobre la solicitud de alta del servicio. Es necesario especificar los datos que se presentan y describen en la Tabla 1.

Dato	Descripción
Nombre del Organismo Solicitante	Nombre del organismo que solicita la publicación del servicio en la PGE (ej. AGESIC, BPS, etc.).
Dependencia	Si es una dependencia de un organismo, indicar su nombre.
Fecha de Solicitud	Fecha en que se realiza la solicitud de publicación del servicio.
Nombre del Solicitante	Nombre completo del funcionario que realiza la solicitud.
Correo Electrónico del Solicitante	Correo electrónico de contacto del funcionario que realiza la solicitud.
Nombre del Responsable Técnico	Nombre del responsable técnico del servicio a publicar.

Correo Electrónico del Responsable Técnico	Correo electrónico del responsable técnico del servicio a publicar.

Tabla 1 – Información General de la Solicitud de Alta de Servicio

Información de Conexión

En esta sección del formulario, el organismo debe proporcionar la información necesaria para la conexión del servidor a la PGE. Se deben especificar los datos que se presentan y describen en la Tabla 2.

Dato	Descripción
Nombre del Nodo de REDuy	Nombre otorgado por AGESIC en el momento de la conexión del organismo a REDuy (ej. AGESIC, BPS, etc.).
Dirección IP Interna del Servidor	Dirección IP interna del servidor del organismo que aloja el servicio a publicar. Es el equipo que recibe los pedidos del firewall de REDuy.
Puerto TCP	Puerto TCP del servidor, en donde el servicio atenderá las peticiones de los clientes.

Tabla 2 – Datos de Conexión del Servidor donde está el Servicio

Estos datos son utilizados por AGESIC para habilitar, en los firewalls de REDuy, el tráfico hacia el servidor donde se encuentra desplegado el servicio.

Solicitud de Certificado para Conexión SSL

En esta sección del formulario, el organismo debe especificar si posee el certificado digital necesario para la conexión SSL y en caso de no poseerlo debe realizar el pedido correspondiente, según lo descrito en la sección "**¡Error! No se encuentra el origen de la referencia.**". Concretamente, se deben indicar los datos que se presentan y describen en la Tabla 3.

Dato	Descripción
¿Posee un certificado digital para dicho servidor?	Indicar si ya fue otorgado un certificado digital para la conexión SSL con el servidor.
Pedido del certificado digital (PKCS#10)	En caso de no poseer certificado, indicar el pedido en formato PKCS#10.

Tabla 3 – Datos de Solicitud del Certificado para la Conexión SSL

Descripción del Servicio

Esta sección del formulario agrupa información relativa al servicio a publicar. Se deben especificar los datos que se presentan y describen en la Tabla 4.

Dato	Descripción
Nombre del Servicio	Nombre del servicio a publicar.
Versión del Servicio	Versión del servicio a publicar.
Nombre del Archivo WSDL	Nombre del archivo descriptor del servicio.
Descripción del Servicio	Descripción general del servicio.
Categorías de Servicio	Categorías del servicio (mínimo 3). Por ejemplo: salud, social, trabajo, general, etc.

Tabla 4 – Datos de Descripción del Servicio

Políticas de Acceso al Servicio

El servicio a publicar por el organismo en la PGE debe especificar las políticas de acceso que define. Las mismas incluyen los perfiles de usuarios que admite, las operaciones a las que cada perfil tiene permitido invocar y cómo se relacionan los perfiles con los roles definidos por los organismos que consumirán dicho servicio.

Perfiles de Usuario

En esta sección del formulario se incluyen los perfiles de usuarios a los que se les permitirá el acceso al servicio. Estos perfiles deben ser definidos por el organismo proveedor del servicio. Se deben especificar los datos que se presentan y describen en la Tabla 5.

Dato	Descripción
Perfil de Usuario	Nombre del perfil de usuario.
Descripción	Descripción del perfil de usuario.

Tabla 5 – Datos de los Perfiles de Usuario Definidos

En la Tabla 6 se presenta un ejemplo de perfiles de usuario definidos para el servicio “Certificados de Nacidos Vivos”.

Perfil de Usuario	Descripción
Admin	Administradores del servicio.
User	Usuarios del servicio.

Tabla 6 – Ejemplo de Definición de Perfiles

Métodos Autorizados por Perfil

Esta sección presenta los métodos del servicio autorizados para cada perfil definido en el punto anterior. Se deben especificar los datos que se presentan y describen en la Tabla 7.

Dato	Descripción
Método del Servicio	Nombre de cada método del servicio
Perfiles autorizados	Perfiles de usuarios autorizados para invocar el método en cuestión

Tabla 7 – Datos de los Métodos Autorizados por Perfil

En la Tabla 8 se presenta un ejemplo de métodos autorizados para los perfiles de usuario definidos en el servicio "Certificados de Nacidos Vivos".

Método del servicio	Perfiles de usuario autorizados
getCertificadosByCriteria	Admin
registrarCNVE	User, Admin

Tabla 8 – Ejemplo de definición de perfiles

Mapeo entre Perfiles de Usuario y Roles Funcionales

En esta sección del formulario se incluyen los métodos del servicio autorizados para cada perfil definido en el punto anterior. Se deben especificar los datos que se presentan y describen en la Tabla 9.

Dato	Descripción
Perfil	Nombre del perfil del usuario definido.
Roles funcionales	Roles funcionales de los clientes, asociados al perfil definido por el servicio.

Tabla 9 – Datos de los Métodos Autorizados por Perfil

En la Tabla 10 se presenta un ejemplo de mapeo entre perfiles de usuario y roles funcionales de los organismos clientes del servicio "Certificados de Nacidos Vivos".

Perfil	Roles Funcionales
Admin	ou=doctor, ou=gerencia de proyectos, o=agesic
User	ou=doctor , ou=prestaciones, o=bps

Tabla 10 – Ejemplo de Mapeo entre Perfiles de Usuario y Roles Funcionales

Configuración Conexión SSL

Como se explica en la sección "**¡Error! No se encuentra el origen de la referencia.**", se debe instalar el certificado raíz de la CA de la PGE en el servidor del organismo donde se aloja el servicio. Además, se deben realizar las tareas de configuración necesarias en el servidor, para posibilitar el establecimiento de la conexión SSL.

Manejo de Invocaciones al Servicio

Como se explica previamente, todas las invocaciones que reciba un servicio de la PGE fueron previamente autenticadas y autorizadas. De esta forma, el único control de acceso que debe realizar el servicio es el de validar el origen de los pedidos.

Asimismo, como se menciona en secciones anteriores, en toda invocación se adjunta un *token* SAML firmado por la PGE, cuya firma es aconsejable que el proveedor valide. Además, el proveedor puede obtener los datos del *token* SAML (por ejemplo, el rol del usuario) para lo que considere necesario.

Comentarios Adicionales

Tecnologías de Implementación

Para seleccionar la tecnología de implementación de los servicios, se pueden tomar en cuenta muchos factores como el ambiente objetivo de instalación y ejecución, experiencia del personal, costos y apoyo de las herramientas de desarrollo. El último punto es importante ya que muchas de las tareas de implementación descriptas en este documento se pueden ver simplificadas dependiendo de la elección realizada.

Ejecución de un Servicio en la PGE

Como se menciona en secciones anteriores, existe la posibilidad de alojar y ejecutar los servicios de los organismos en la PGE, si éstos tienen algún requerimiento que no es posible cumplir en los servidores de los organismos.

En el caso que un organismo quiera solicitar alojamiento en la PGE para un servicio, debe enviar un correo electrónico a la dirección soporte@agesic.gub.uy, especificando en el asunto del correo "[Ejecución de un Servicio en la PGE] *Nombre del Organismo Proveedor*". Se debe brindar además información sobre el servicio a publicar y sobre los motivos por los cuales se requiere su ejecución en la PGE. Una vez recibido el formulario se coordinará una entrevista con el personal de AGESIC.

Los servicios a ejecutarse en la PGE tienen el requerimiento extra de que deben poder desplegarse y ejecutarse en alguno de los entornos de ejecución provistos por la misma.

Consumo de un Servicio en la PGE

Prerrequisitos

Para que un organismo pueda consumir un servicio de la PGE es necesario que tenga conexión a la REDuy.

A su vez, es necesario que se den de alta en el directorio de la PGE, los roles del organismo que consumirán los servicios. Como se explicó previamente cada organismo administrará su rama del árbol de roles.

Completar y Enviar Formulario para el "Consumo de Servicios"

El organismo que quiera consumir servicios de la PGE debe completar y enviar a AGESIC el "**¡Error! No se encuentra el origen de la referencia.**". Dicho formulario requiere información general e información para la conexión del organismo consumidor con la PGE. El formulario debe ser enviado por correo electrónico a la dirección soporte@agesic.gub.uy, especificando en el asunto del correo "[Consumo de Servicios de la PGE] Nombre del Organismo Cliente". En las próximas sub-secciones se describe la información que se debe incluir en este formulario.

Información General de la Solicitud

En primer lugar, el organismo debe brindarle a AGESIC información general sobre la solicitud para el consumo de servicios. Es necesario especificar los datos que se presentan y describen en la Tabla 11.

Dato	Descripción
Nombre del Organismo Solicitante	Nombre del organismo que solicita el consumo de servicios en la PGE (ej. AGESIC, BPS, etc.).
Dependencia	Si es una dependencia de un organismo, indicar su nombre.
Fecha de Solicitud	Fecha en que se realiza la solicitud de consumo de servicios.
Nombre del Solicitante	Nombre completo del funcionario que realiza la solicitud.
Correo Electrónico del Solicitante	Correo electrónico de contacto del funcionario que realiza la solicitud.
Nombre del Responsable Técnico	Nombre del responsable técnico de la aplicación cliente.
Correo Electrónico del Responsable Técnico	Correo electrónico del responsable técnico de la aplicación cliente.

Tabla 11 – Información General de la Solicitud de Consumo de Servicios

Información de Conexión

En esta sección del formulario, el organismo debe proporcionar la información necesaria para la conexión con la PGE. Se deben especificar los datos que se presentan y describen en la Tabla 12.

Dato	Descripción
Nombre del Nodo de REDuy	Nombre otorgado por AGESIC en el momento de la conexión del organismo a REDuy (ej. AGESIC, BPS, etc.).
Dirección IP interna del cliente	Dirección IP interna de la aplicación cliente.

Tabla 12 – Datos de Conexión para el Cliente

Solicitud de Certificado para Conexión SSL

En esta sección del formulario, el organismo debe especificar si posee el certificado digital necesario para la conexión SSL y en caso de no

poseerlo debe realizar el pedido correspondiente, según lo descrito en la sección "**¡Error! No se encuentra el origen de la referencia.**". Concretamente, se deben indicar los datos que se presentan y describen en la Tabla 13.

Dato	Descripción
¿Posee un certificado digital para dicho cliente?	Indicar si ya fue otorgado un certificado digital para la conexión SSL.
Pedido del certificado digital (PKCS#10)	En caso de no poseer certificado, indicar el pedido en formato PKCS#10.

Tabla 13 – Datos de Solicitud del Certificado para la Conexión SSL

Configuración Conexión SSL

Como se explica en la sección "**¡Error! No se encuentra el origen de la referencia.**", se debe instalar el certificado raíz de la CA de la PGE en el servidor o computador donde se aloja la aplicación cliente. Además, se deben realizar las tareas de configuración necesarias para posibilitar el establecimiento de la conexión SSL.

Obtener Descripción del Servicio

La PGE proveerá un Registro UDDI para la búsqueda y descubrimiento de servicios. El resultado de las búsquedas brindará información general de los servicios y la ubicación del WSDL que los describe.

Implementar Aplicación Cliente

Una aplicación cliente en un organismo debe realizar tres pasos para consumir un servicio de la PGE:

1. obtener un *token* de seguridad firmado por el organismo
2. obtener un *token* de seguridad firmado por la PGE
3. invocar al servicio

En las próximas sub-secciones se describen estos pasos, especificando los estándares que se utilizan y la información que se envía y recibe en cada uno de ellos.

Obtener *token* de Seguridad SAML firmado por el Organismo

El primer paso que debe realizar una aplicación cliente para invocar un servicio de la PGE, es obtener un token de seguridad SAML (v 1.1 o 2.0) firmado digitalmente por el organismo. En casos en que el organismo no cuente con una aplicación emisora de tokens, puede utilizar la Librería de Ejemplo implementada por AGESIC para desarrollar una.

Importante: La librería fue desarrollada como prueba de concepto, por lo cual no está garantizada la ausencia de errores, ni fallas de seguridad. No se recomienda entonces utilizarla en producción, sin los resguardos apropiados según las políticas de testing y seguridad de cada organismo.

La emisión de un token SAML por el organismo, implica que el usuario está autenticado y que su información enviada en el token es válida. La firma del token es el mecanismo utilizado para garantizar la autenticidad del pedido e integridad de la información presentada. El token SAML debe incluir la información descrita en la Tabla 14.

Dato	Descripción
Rol	Rol del cliente dentro del organismo. Se debe especificar a través del DN de la entrada en el directorio LDAP del organismo. Por ej.: “ou=medicos, o=msp”.
Usuario	Nombre de usuario que está ejecutando la aplicación. Este atributo es utilizado con fines de auditoría y no participa en los procesos de autenticación y autorización de la PGE. Queda a criterio del organismo el valor a utilizar.

Tabla 14 – Datos a del *token* de Seguridad SAML a emitir por el Organismo Cliente

En el Apéndice 3 se presenta un ejemplo simplificado de un token SAML generado y firmado por un organismo, mostrando cómo ubicar los elementos presentados en la Tabla 14.

Obtener un *token* de Seguridad SAML firmado por la PGE

El segundo paso que debe realizar una aplicación cliente, es obtener un token de seguridad firmado por la PGE. Para ello debe realizar una solicitud al STS de la PGE utilizando el estándar WS-Trust (versión 1.3). La Tabla 15 describe los datos que debe incluir la solicitud.

Dato	Descripción
Token SAML	*Token* de seguridad SAML (versión 1.1 o 2.0) con información del cliente y firmado por el organismo.
PolicyName	Política de autenticación utilizada por AGESIC para la verificación de solicitudes del cliente. Los posibles valores para este atributo son definidos por la AGESIC. Actualmente el único valor posible es "urn:simpletoken)".
Tipo de *token* a solicitar	Este valor indica el tipo de *token* que se solicita. Actualmente la PGE acepta la emisión de *tokens* SAML versión 1.1.
Servicio	Dirección lógica del servicio de la PGE a consumir.

Tabla 15 – Datos a incluir en el RST

En el Apéndice 3 se presenta un ejemplo simplificado de un mensaje RST, mostrando cómo ubicar los elementos presentados en la Tabla 15 mediante el uso del estándar WS-Trust.

El STS verifica la firma del token SAML y la existencia del rol en la PGE y emite un token de seguridad SAML firmado por la PGE con los datos presentados en la Tabla 16.

Dato	Descripción
Rol	Rol del cliente dentro de la PGE. Se debe especificar a través del Distinguished Name (DN) de la entrada en el directorio LDAP de la PGE. Por ejemplo: "ou=medicos, o=msp, ……,c=uruguay.
Usuario	Nombre de usuario. Este atributo es utilizado con fines de auditoría y no participa en los procesos de autenticación y autorización de la PGE.
PolicyName	Política de autenticación utilizada por AGESIC para la verificación de solicitudes del cliente.
Servicio	Dirección lógica del servicio de la PGE a consumir.

Tabla 16 – Datos incluidos en el token emitido por el STS

En el Apéndice 3 se presenta una versión simplificada de este token, mostrando la ubicación de los elementos de la Tabla 16.

Invocar al servicio

Por último, para invocar un servicio de la PGE, la aplicación cliente debe enviar un mensaje SOAP al Servicio Proxy del servicio con la siguiente información:

1. *token* SAML emitido por el STS de la PGE, especificado a través del estándar WS-Security, versión 1.1.

2. servicio y método a consumir, especificados a través de estándar WS-Addressing versión 1.0.

3. información de negocio de acuerdo al WSDL del servicio

En el Apéndice 3 se presenta un ejemplo simplificado de un mensaje SOAP para consumir el servicio "Certificado de Nacidos Vivos" utilizando los estándares WS-Addressing y WS-Security con la información mencionada anteriormente.

Comentarios Adicionales

Tecnologías de Implementación

Muchas de las tareas de implementación para el consumo de servicios se pueden ver simplificadas dependiendo de las herramientas de desarrollo que se utilicen.

Referencias

[1] Basic Profile. http://www.ws-i.org/Profiles/BasicProfile-1.1.html [Accedida en Mayo de 2010]

[2] Basic Security Profile. http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.tml [Accedida en Mayo de 2010]