DIR3 - Securización servicios

Normalización securización de los servicios web

Versión: 0100

Fecha:27/10/2014

[1.0.0.0]

HOJA DE CONTROL

Organismo	**Consejería de Hacienda y Administración Pública**		
Proyecto	DIR3 - Securización servicios		
Entregable	Normalización securización de los servicios web		
Autor	Servicio de Coordinación y Desarrollo de Sistemas Horizontales		
Aprobado por		**Fecha Aprobación**	
		Nº Total de Páginas	13

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
0100	Versión inicial	Srv. de Coord. y Desarrollo de Sistemas Horizontales	27/10/2014

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos
Juan Sebastián Ojeda Pérez (SCDSH)
Jorge Sanchez(SCDSH)
Antonio Blanco Morales (SCDSH)
Juan Antonio Campano Berlanga (SANDETEL)

1 INTRODUCCIÓN

DIR3 (también llamado Directorio Común), es un servicio web integrable en aplicaciones cliente, publicado dentro de la red SARA, que proporciona un inventario unificado y común a toda la Administración de las unidades orgánicas/organismos públicos, sus oficinas asociadas y unidades de gestión económica-presupuestaria, facilitando el mantenimiento distribuido y corresponsable de la información.

Consta de una serie de servicios, cuyo ambito funcional se puede resumir en:

- **Consumo y provisión de información**, para todos los usuarios con acceso al sistema del sistema de información, a través de sus diferentes mecanismos. Asimismo, el Directorio es responsable de la creación y mantenimiento de la codificación única de las unidades y oficinas.

- **Gestión de usuarios**, asociados a perfiles y ámbitos de administración.

- **Calidad y alertas**, personalizables por usuario.

Poseen un mecanismo de autenticación no estandarizado, consistente en introducir las credenciales en campos dentro del cuerpo de la petición SOAP.

El servicio, no esta publicado bajo protocolo seguro (HTTPS).

En el presente documento se indican las acciones realizadas para securizar el servicio WEB utilizando la infraestructura de Platina, así como otras configuraciones realizadas para garantizar la total trazabilidad de las invocaciones realizadas al servicio.

PLATINA

Las siglas PLATINA corresponden a la PLATaforma de INteroperabilidad de la Junta de Andalucía. Podríamos definir la Interoperabilidad (técnica) como la "capacidad de diferentes productos y servicios de TI para intercambiar y usar datos e información (es decir "hablar"), con el objetivo de funcionar juntos en un entorno conectado en red".

El proyecto PLATINA es una plataforma tecnológica SOA que facilita e implanta un modelo común de interoperabilidad técnica en la Administración de la Junta de Andalucía y que permite servir como infraestructura de soporte común para facilitar la integración e interoperabilidad entre servicios de la Junta de Andalucía y de distintas Administraciones.

A modo informativo y de forma resumida, describimos los productos implicados en PLATINA:

Módulo	Descripción	Abreviatura
Bus de servicio	Se trata de Bus de Servicio de Empresa (WSO2 ESB) de código abierto, rápido, ligero y fácil de usar. Está basado en el motor de mediación Apache Synapse. Permite principalmente el enrutamiento de mensajes, la mediación, transformación, trazabilidad, programación de tareas, enrutamiento por error, balanceo de carga y otras funcionalidades más avanzadas.	**ESB**
Repositorio	Es una implementación de código abierto (WSO2 Government Registry) de un registro-repositorio SOA. Proporciona un completo repositorio de meta-datos y permite la gestión	**GREG**

	completa de versiones de servicios, la gestión de su ciclo de vida, un modelo de administración basado en usuarios, roles y permisos, y otras características, tales como el etiquetado, la clasificación y comentarios. Todo gestionable a través de la interfaz de usuario basada en web.	
Servidor de Identidad	Se trata de un componente para la gestión de identidad y de permisos basado en código abierto (WSO2 Identity Server) y que tiene soporte para OpenID, tarjetas de información (Information Card), XACML y SAML 2.0.	**IS**
Monitor de actividad de negocio	BAM es el componente basado en software libre (WSO2 BAM) de la plataforma que se encarga de la monitorización de métricas SOA, de indicadores clave de negocio que hayan sido definidos y cualquier otro parámetro que sean medibles. La información que ofrece este herramienta tiene como objetivo principal cubrir las necesidades de monitorización y compresión de las actividades que se desarrollan en el organismo, tanto desde un punto de vista de negocio como desde el ámbito de la tecnología de la información (TI).	**BAM**
Message Broker	Componente que ofrece soporte para arquitecturas dirigidas por eventos. Este componente está basado en Apache Qpid que es un referente de hoy día en la ingeniería de mensajes. MB permite el acceso unificado y simultáneo a la mensajería mediante diversos protocolos, tales como JMS,WS-Eventing, Amazon SQS y AMQP.	**MB**
Servicios Datos	Este componente puede interactuar con múltiples fuentes de datos y exponer la información como servicios web.	**DSS**

2 Securización de los Servicios Web DIR3

El servicio de Directorio Común (DIR3), consta de una serie de servicios publicados dentro de la Red SARA. De todo el catalogo de servicios, se solicitó realizar un estudio y posterior implementación para securizar tres servicios concretos (los de consumo):

- **Volcado de Catalogo:** descarga de los catálogos exportables existentes en el nuevo Directorio Común (DIR3), en formato fichero, en base a unos criterios definidos. Se permitirá la descarga tanto de catálogos básicos como del total de ellos.

- **Descarga Unidades**: descarga de los datos de unidades orgánicas del directorio común (en formato fichero). De forma subordinada, se presenta la posibilidad de descargar los datos acotados mediante unos filtros, definidos posteriormente. Se descargarán tanto los datos de las unidades orgánicas como los datos derivados de la gestión del cambio de extinciones y de anulaciones de las mismas.

- **Descarga Oficinas**: descarga de los datos de oficinas del directorio común (en formato fichero), en base a unos criterios determinados. Se podrán descargar los datos de las oficinas, las relaciones entre oficinas y unidades y la gestión de extinciones y de anulaciones de las mismas (históricos). Cuando se descargan las relaciones entre unidades y oficinas hay que tener en cuenta :

    - ***Descarga normal:*** Si se indica el estado vigente (V), solo se devolverán las relaciones con unidades vigentes.

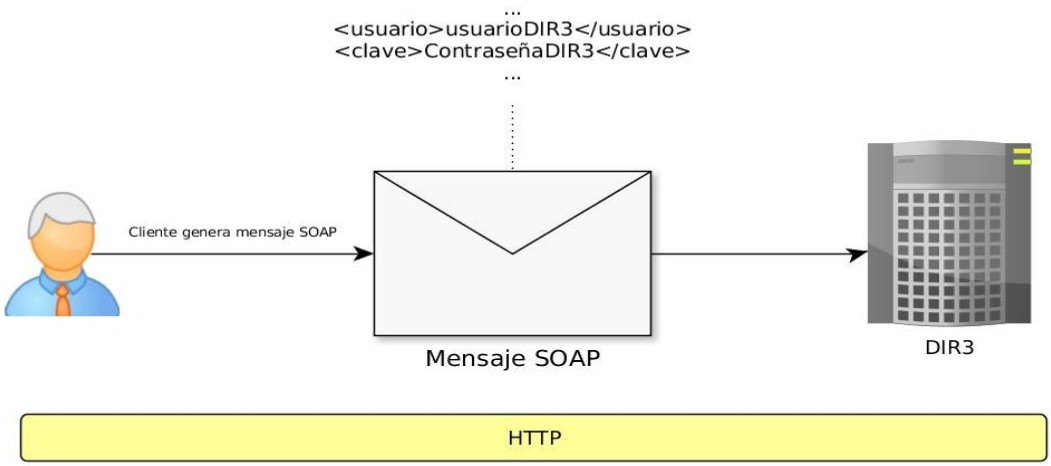
    - ***Descarga incremental:*** Si se indica estado vigente (V), se devolverán todas las relaciones vigentes y las extinguidas que estén dentro del rango de fechas especificados.

Los servicios anteriormente descritos, se encuentran publicados bajo protocolo no seguro (HTTP) . Las URL son las siguientes:

- http://dir3ws.redsara.es/directorio/services/SC21CT_VolcadoCatalogos?wsdl
- http://dir3ws.redsara.es/directorio/services/SD02OF_DescargaOficinas?wsdl
- http://dir3ws.redsara.es/directorio/services/SD01UN_DescargaUnidades?wsdl

Para poder hacer consumo de dichos servicios, es necesario disponer de unas credenciales (usuario y contraseña). Dichas credenciales viajan en claro, como cualquier otro parámetro, en el cuerpo del mensaje SOAP, sin seguir ninguna especificación concreta.

Se utilizan las mismas credenciales para todas las aplicaciones que se integran, no teniendo posibilidad de utilizar credenciales diferenciadas para cada aplicación.



2.1 Solución propuesta

Para realizar la securización de los servicios, se propone la siguiente solución tecnológica:

- Implementar un proxy por cada servicio en el componente BUS de PLATINA (WSO2 ESB). Dicho proxy, implementará las siguientes medidas:

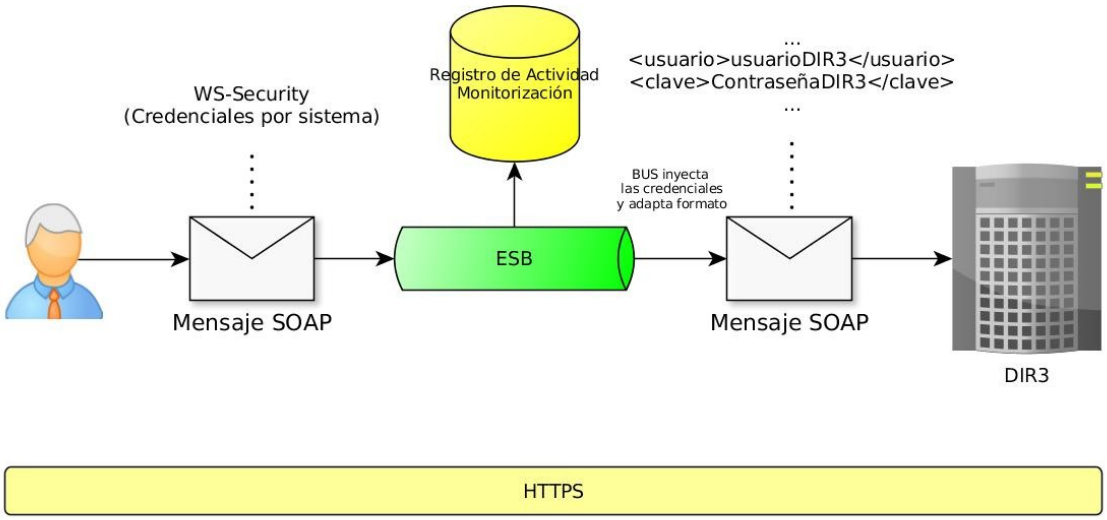
    - Se utilizará únicamente un transporte seguro para el consumo de los servicios. Entre el cliente del servicio y el BUS, la comunicación siempre será cifrada, reduciendo el riesgo de que se pueda obtener información de los mensajes intercambiados, mediante ataques dirigidos.

    - Se utilizará el protocolo WS-Security (WSS), que suministra un medio para aplicar seguridad a los Servicios Web.

    - Se expondrá un nuevo contrato de servicio, donde desaparecerán los campos utilizados para la autenticación (usuario y contraseña). Dichos campos serán inyectados directamente por el BUS al recibir las peticiones. De esta forma, los clientes no conocen las credenciales utilizadas para DIR3, solo necesitaran autenticarse contra el BUS para consumir el servicio.

    - Se utilizará credenciales diferenciadas por aplicación.

- Se implementará mecanismos de monitorización en BAM, con el fin de obtener trazas completas de las comunicaciones que circulan por el BUS, así como de los errores producidos.



2.2 Implementación de la solución propuesta

Para implementar la solución, se ha hecho uso de la infraestructura existente en PLATINA, basada en productos de WSO2. En concreto, se han diseñado tres proxys de servicio, dentro del BUS de Servicios, que realizan las tareas de mediación/transformación necesarias sobre los mensajes para adaptarlos a las necesidades descritas en la solución.

Adicionalmente, mediante configuración sobre la herramienta, se pueden activar fácilmente mecanismos de caché o control de flujo sobre los servicios desarrollados, para optimizar la forma en que estos son consumidos.

Como entregables de dicha implementación, se han generado 3 paquetes listos para desplegar en el Bus de Servicios:

- DIR3DESCARGAUNIDADESWS_1.0.0.car
- DIR3VOLCADOCATALOGOWS_1.1.0.car
- DIR3DESCARGAOFICINASWS_1.0.0.car

Que habilitarían los endpoints correspondientes para las integraciones.