Construcción de un módulo de seguridad integrado en una arquitectura SOA Open Source

Víctor Ayllón, Juan Manuel Reina
NOVAYRE - www.novayre.es
C/Leonardo Da Vinci 18, 5ª Planta
Parque Tecnológico Cartuja - 41092 Sevilla - Teléfono: 954 463 108
{vayllon, jmreina}@novayre.es

Resumen. La Fundación Progreso y Salud, FPS, dependiente de la Consejería de Salud de la Junta de Andalucía, es el organismo de apoyo y gestión a la investigación en la sanidad pública andaluza. En los últimos años la FPS está encarando un proceso de definición y fortalecimiento de su arquitectura técnica basándose en una arquitectura orientada a servicios (SOA), que le permite disponer de una infraestructura de interoperabilidad entre los distintos sistemas de información que forman parte de su extenso catálogo de aplicaciones. Para poder disponer de una infraestructura SOA se necesitan un conjunto de módulos comunes y reutilizables orientados a proporcionar funcionalidad de soporte, no directamente relacionada con la lógica de negocio de las aplicaciones. Entre estos servicios transversales destacan los relativos a la seguridad de las aplicaciones, en particular los sistemas Single Sign-On (SSO). En este documento se presenta la solución SOA proporcionada por NOVAYRE para el diseño y construcción del módulo de seguridad SSO.

Keywords: SOA, SSO, CAS, Open Source, LDAP, Spring, Novayre, Web Services, JAX-WS

1 Antecedentes

Las organizaciones tienen la necesidad de simplificar el proceso de creación y desarrollo de nuevas aplicaciones, así como de fomentar la reutilización mediante el uso de servicios compartidos en varios procesos de negocio.

Las Arquitecturas Orientadas a Servicio (SOA) son un paradigma software que promueven el empleo coordinado de un conjunto de servicios reutilizables, débilmente acoplados entre sí, para dar soporte a los requerimientos de negocio.

En este contexto, la Fundación se planteó diseñar un enfoque SOA para abordar sus nuevos retos tecnológicos, entre los que se encontraba el desarrollo de un módulo de seguridad con capacidad SSO que centralizara el acceso a todas las aplicaciones. Un sistema SSO permite "transportar" la información de autenticación de un sistema a otro. Si no se implantara una solución de este tipo los usuarios estarían obligados a autenticarse en cada una de las aplicaciones del sistema. Este hecho provocaría la pérdida de tiempo en estos procesos de autenticación y también disminuiría la

“usabilidad”. En lugar de esto, los sistemas SSO nos permiten centralizar los procesos de autenticación reduciendo así el número de autenticaciones.

2 Problema a resolver

El problema a resolver consiste en crear un único módulo de autenticación y seguridad con funciones SSO que centralice la administración de usuarios, en concreto las funciones de alta/baja/modificación de usuarios en el ERP corporativo, accediendo a su vez a la arquitectura SOA planteada por Novayre para resolver la problemática asociada al acceso a entidades comunes de la FPS (Centros de Trabajo, Localización, Personas, etc.)

Asimismo este módulo debería integrarse con los sistemas de autenticación de la FPS (concretamente con LDAP) facilitando considerablemente el cumplimiento de las políticas de seguridad establecidas al ser el único punto de acceso para el registro y autenticación de los usuarios.

Por último este módulo se debería construir utilizando únicamente soluciones Open Source.

3. Solución propuesta

La solución proporcionada por Novayre (figura 1) fue el desarrollo de un módulo de Seguridad que permite disponer de un control centralizado (conocido como las tres Aes):

- Autenticación
- Autorización
- Auditoría de accesos

Fig. 1. Módulo de Seguridad

El módulo fue construido únicamente utilizando soluciones Open Source, destacando Central Authentication Server - CAS para la autenticación centralizada y apoyándose en su implementación en las librerías de Spring y JAX-WS.

La arquitectura técnica diseñada es la siguiente (figura 2).

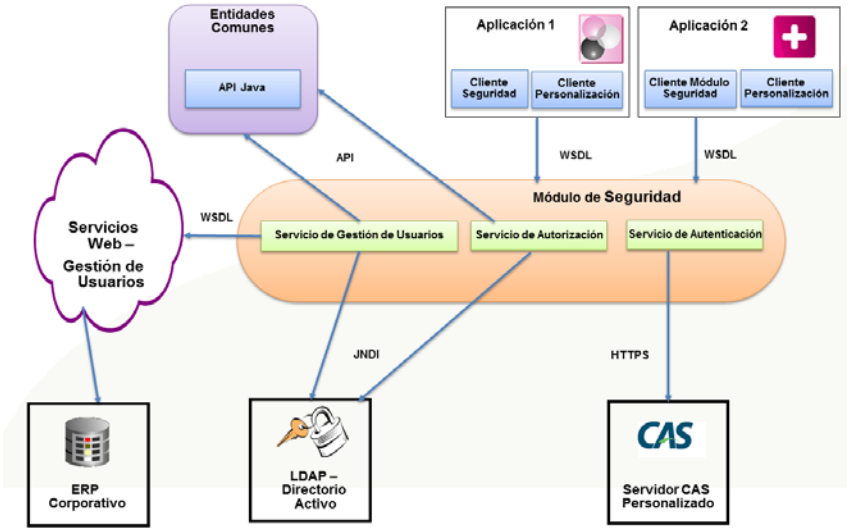

Fig. 2. Arquitectura técnica de la solución

Entre otros componentes, destacan:

Servicio de Gestión de Usuarios: permite realizar las funciones de gestión de usuarios (alta/consulta/modificación) de una forma uniforme integrándose vía Web Services con el ERP corporativo vía JNDI con LDAP

Servicio de Autorización: gestiona la autorización a las aplicaciones en base a los perfiles establecidos

Servicio de Autenticación: gestiona la autenticación única al sistema invocando a un servidor CAS personalizado y adaptado a las necesidades del proyecto. Este servidor dispone de varias páginas de login personalizadas que permiten la autenticación a través de usuario y contraseña, validando los datos en LDAP. Estas distintas versiones de las páginas de login permiten mostrar al usuario información de contexto en función de la aplicación donde se está requiriendo la autenticación, de esta forma, es posible mostrar para algunas aplicaciones que el usuario debe realizar la operación de login, mientras que en otras se muestra la página de login contextualizada para la aplicación. Este servicio también gestiona el logout único e integrado de forma que el usuario sólo debe realizar dicha operación para una aplicación propagándose este estado a las demás aplicaciones del sistema.

Aplicaciones: aplicaciones de la FPS con las que se integra el módulo de seguridad. El acceso a dicho módulo se realiza, por un lado vía un módulo Java (cliente de seguridad) desarrollado ad-hoc para facilitar la invocación de los servicios

web. Se desarrollaron dos versiones del cliente de seguridad para Java, uno para clientes legacy (Spring 2.X) y otro para clientes que utilizan Spring 3.X. Asimismo proporcionamos una configuración específica que facilita la integración de las aplicaciones Java con el sistema SSO (cliente de personalización).

Módulo de Entidades Comunes: establecido como único punto de acceso a aquellas entidades que son comunes a todas las aplicaciones de la FPS. Este módulo, construido en parte con el generador de código de Novayre - Gator™- se diseñó con una arquitectura "dual", es decir, construyendo un API Java (librería) que encapsula el acceso a los servicios para las aplicación Java y exportando a su vez los servicios vía Web Services para aplicaciones no escritas en lenguaje Java. En la siguiente imagen (figura 3) se muestra la arquitectura "dual":

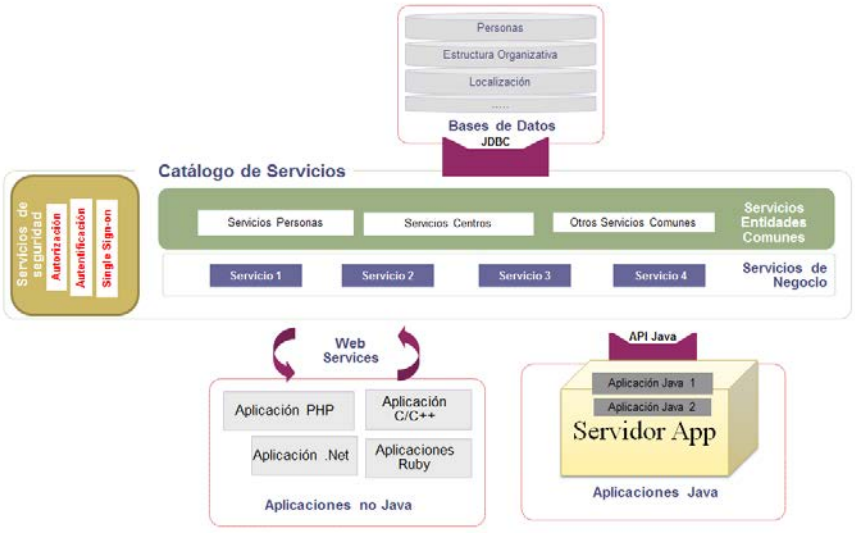

Fig. 3. Modelo de integración

Asimismo, otra consideración técnica fue la necesidad de añadir al servidor de CAS personalizado una función de "autologin" fruto de la necesidad por parte de la FPS de que existiera una página de autenticación diferente a la que proporciona CAS y que se ubica físicamente en otra aplicación web.

Esta función de "autologin" permite autenticarse en CAS proporcionando, desde una aplicación externa, las credenciales (usuario y contraseña). Además de utilizar funciones de encriptación para la comunicación con CAS, se implementó una marca de tiempo para impedir accesos no autorizados. Esta marca de tiempo implica que los links generados para el "autologin" tienen una caducidad determinada (20 segundos) lo que impide que un usuario que pueda recuperar el enlace (por ejemplo utilizando el historial del navegador) pueda acceder al sistema.

4. Conclusiones

Novayre tiene un importante reconocimiento público en la ejecución de proyectos de alto riesgo tecnológico y elevada complejidad. Durante estos años hemos conseguido sostener una diferenciación considerable a través de nuestra reputación en terminar proyectos complejos en el tiempo previsto. Nuestras capacidades nos llevan a que habitualmente se nos solicite para colaborar en proyectos de “alto impacto”, por su enfoque estratégico, su visibilidad, su complejidad tecnológica o su influencia directa en resultados.

El enfoque SOA proporcionado por Novayre es un proyecto de “alto impacto” que ha permitido a la Fundación abordar los nuevos desafíos tecnológicos. En particular, la construcción de este módulo hace que los usuarios de la Fundación dispongan de un único identificador para el acceso a todas las aplicaciones corporativas y externas facilitando una experiencia de Single Sign-On (SSO) para los usuarios. Este módulo evita duplicidades en la gestión de usuarios, facilitando a su vez la reutilización de los activos existentes y la flexibilidad en los cambios. Asimismo, el disponer de un único punto de acceso a las aplicaciones aumenta la usabilidad de los sistemas ya desarrollados y como no, la propia satisfacción de sus usuarios.