Integración de aplicaciones SAML 2.0 (SSOWeb)

Manual de integración

Versión: 0100

[Versión del Producto]

HOJA DE CONTROL

Organismo	Sandetel		
Proyecto	Single Sign On Web		
Entregable	Manual de integración		
Autor	Francisco Rodríguez Corredor		
Aprobado por		**Fecha aprobación**	08/10/2019
		Nº total de páginas	11

REGISTRO DE CAMBIOS

Versión	Causa del cambio	Responsable del cambio	Fecha del cambio
3.0	Guía de integración con SSOWeb utilizando spring- security-saml	Francisco Rodríguez Corredor	13/02/2018
3.1	Actualización urls recursos, servicio NAOS	UPSH	08/10/2019
4.0	Actualización por el cambio de tecnología de OpenAM a adAS	Fernando Piedra de la Cuadra	05/05/2020

CONTROL DE DISTRIBUCIÓN

Nombre y apellidos

ÍNDICE

1 OBJETIVO

El objetivo del presente documento es servir de guía para el desarrollo de integraciones de aplicaciones J2EE que quieran hacer uso de las funcionalidades disponibles en el sistema Single Sign On Web.

1.1 Audiencia

El documento está dirigido a los desarrolladores de aplicaciones J2EE que requieran integrar en sus aplicaciones la autenticación vía Single Sign On Web.

1.2 Glosario y definiciones

- SSO (Single Sign On). Es un mecanismo de autenticación mediante el cuál el usuario se autentica una vez propagando la identidad a las aplicaciones
- SAML. Es un estándar basado en XML para el intercambio de mensajes de autenticación y autorización entre dominios de seguridad.
- Federación de Identidades. La identidad federada es una de las soluciones para abordar la gestión de identidad en los sistemas de información. Su objetivo es obtener una gestión de usuarios eficiente, la sincronización de los datos identificativos, gestión de acceso, servicios de agrupación, servicios de directorio, auditoria e informes
- SP (Service Provider). Es el elemento que consume la información de autenticación y autorización en la relación federada. Se puede equiparar a la aplicación de negocio a integrar.
- IDP (IDentity Provider). Es el elemento que contiene la información de origen de la identidad en una relación federada.

2 PROCESO DE INTEGRACIÓN

2.1 Requisitos para la integración con Single Sign On Web

A continuación se enumeran los requisitos para la integración en el SP:

- Entorno JAVA:
  - JDK: **versiones 1.6, 1.7 y 1.8**
  - Servidor de aplicaciones J2EE.
  - Permisos para reiniciar el servidor de aplicaciones.
- El servidor debe tener configurada y operativa la resolución por DNS (FQDN).

2.2 Procedimiento de configuración e integración

1. Solicitar el alta de la aplicación en NAOS. Acceda al Portal de Usuario de NAOSv3 y solicite el alta mediante un ticket(*) del servicio "Servicios TIC", operación "Realizar petición", componente "Otros", elemento "Single Sign On Web"

   Al ticket NAOS deberá adjuntar el fichero de metadatos que el plugin de SAML generará de forma automática una vez ejecute el punto 11 de este mismo apartado.

   (*) Si no tuviera visibilidad de alguna de las categorías anteriores, puede solicitarla a través de un correo a ceis.soporte.chie@juntadeandalucia.es, desde donde le darán más instrucciones.

2. Integración de los ficheros y recursos necesarios en el WAR de la aplicación a integrar.

   ➔ Descomprima el archivador SAML2-SDK.zip descargado de la ruta:
   https://redprofesional.juntadeandalucia.es/file/view/38464492/saml2-sdkzip

   ➔ Copie el contenido descomprimido en el WAR de la aplicación que desea integrar. Se recomienda realizar el copiado con un comparador de carpetas para resolver los conflictos de librerías que puedan
   surgir y para facilitar la mezcla de los ficheros web.xml y securityContext.xml que posiblemente ya existan el WAR de su aplicación.

3. Si desea utilizar un certificado no autogenerado por la aplicación para cifrar las peticiones SAML recurra al apartado "8.1 Key management" de la Guía oficial del plugin spring-security-saml

(https://docs.spring.io/spring- security-saml/docs/current/reference/html/security.html). Los certificados autogenerados por la aplicación son útiles para entornos de desarrollo pero no deben ser utilizados en entornos productivos. En caso de configurar un certificado distinto al autogenerado debe seguir estando registrado en el almacen de certificados configurado en el fichero securityContext.xml con el alias "apollo".

4. Edite en el securityContext.xml la entrada <security:user name="admin" password="admin" authorities="ROLE_ADMIN"/> y cambiar la password por la que se desee.
5. Edite el fichero securityContext.xml y descomente la configuración existente entre los comentarios <!-- COMIENZO DEL BEAN DE CONFIGURACIÓN PARA UTILIZAR SSOWEB --> y <!-- FIN DEL BEAN DE CONFIGURACIÓN PARA UTILIZAR SSOWEB -->
6. Seleccione el entorno que quiere utilizar para la integración, para ello debe sustituir la cadena "/metadata/ssowebIntegracion.xml" por el valor de la siguiente tabla que se corresponda con el entorno deseado:

Entorno de preproducción	/metadata/adasSSOPreproduccion.xml
Entorno de producción	/metadata/adasSSOProduccion.xml

7. Reinicie el servidor de aplicaciones.
8. Acceda la url http://<nombre_de_la_maquina>:<puerto>/<contexto>/saml/web/metadata y loguese en el formulario de autenticación mostrado.
9. Pulse en "Metadata Administration" y posteriormente en el botón "Generate new service provider metadata".
10. Rellene los siguientes datos en el formulario:
    1. Store for the current session: No
    2. Entity ID: saml.<url_de_la_aplicación> ó nombre identificativo de la misma.
    3. Entity base URL: verificar que la url generada tiene el nombre de dominio correcto para la aplicación.
    4. Entity alias: dejar vacío.
    5. Signing key: NO modificar este campo.
    6. Encription key: NO modificar este campo.
    7. Signature Security Profile: MetaIOP
    8. Resto de valores: NO modificar este campo.
    9. En "Single sing-on bindings" marcar como "default" la opción "SSO HTTP-POST" y su checkbox es el único que debe quedar marcada en la columna "Included".
    10. En "Supported NameIDs" sólo marcar el checkbox "Transient" 11.En "Enable IDP discovery profile" seleccionar "No".
    11. En "Enable IDP discovery profile" seleccionar "No".

11. Tras esto pulse en "Generate metadata" y siga las instrucciones que se indican en la página de resultado para configurar los metadatos y que serán del tipo:

    1. Store metadata content inside your achive at /WEB- INF/classes/metadata/<filename>.xml

    2. Make sure to update your identity provider(s) with the generated metadata.

    3. Modify bean "metadata" in your securityContext.xml and include content from the configuration above.

12. Básicamente los subapartados del punto anterior indican que lo que hay que hacer es:

    1. copiar el contenido del textarea metadata y almacenarlo en un fichero xml llamado <filename>.xml dentro de la carpeta /WEB- INF/classes/metadata de nuestro WAR.

    2. editar el fichero securityContext.xml ubicado en la carpeta WEB-INF de nuestro WAR e incluir en el mismo el contenido del segundo textarea a continuación de la línea "<!--INSERTE A CONTINUACIÓN DE ESTA LÍNEA LA CONFIGURACIÓN DE LOS METADATOS GENERADOS -→"

13. Una vez hecho esto reinicie el servidor de aplicaciones.

2.3 Verificación de la configuración

Puede probar el funcionamiento de la integración accediendo a alguna de la siguiente url https://FQDN:PUERTO/

CONTEXTO/saml/login?idp=SELECTEDIDP

Donde debe sustituir:

- FQDN: nombre de dominio asociado a la aplicación integrada.
- PUERTO: puerto en el que se presta el servicio en la aplicación integrada.
- CONTEXTO: contexto en el que se encuentra desplegada la aplicación integrada.
- SELECTEDIDP: identificador del proveedor de identidades contra el que se desea realizar la autenticación. Deberá seleccionar su valor de la siguiente tabla en función del entorno que desea utilizar:

Single Sign On Web	Entorno de preproducción	https://ssoweb.pre.juntadeandalucia.es/opensso
Single Sign On Web	Entorno de producción	https://ssoweb.juntadeandalucia.es/opensso

2.4 Invocar el proceso de autenticación y procesar la respuesta desde su aplicación

Para invocar el proceso de autenticación desde su aplicación basta con que incluya un enlace con una url con el formato descrito en el apartado anterior.

Mediante las siguientes instrucciones pueden recuperarse los atributos relativos a la identidad del usuario autenticado:

```
<%      Authentication authentication = SecurityContextHolder.getContext().getAuthentication(); if
(authentication != null){
SAMLCredential credential = (SAMLCredential) authentication.getCredentials();
pageContext.setAttribute("authentication", authentication); pageContext.setAttribute("credential",
credential); pageContext.setAttribute("assertion",
XMLHelper.nodeToString(SAMLUtil.marshallMessage(credential.getAuthenticationAssertion())));
} %>
[.....]
[.....]
[.....]
<c:forEach var="attribute" items="${credential.attributes}">
  <tr>
    <td width="200">
         <strong><c:out value="${attribute.name}"/></strong>
         <c:if test="${not empty attribute.friendlyName}"> (<c:out value="$
{attribute.friendlyName}"/>)</c:if>
    </td>
    <td>
    <%
         Attribute a = (Attribute) pageContext.getAttribute("attribute");
         String[] attributeValues = credential.getAttributeAsStringArray(a.getName());
          pageContext.setAttribute("attributeValues", attributeValues);
     %>
    <c:forEach var="attributeValue" items="${attributeValues}">
      <c:out   value="${attributeValue}"/> 
    </c:forEach>
   </td>
  </tr>
</c:forEach>
```

Para más detalles consulte el fichero MyPage.jsp incluido en el fichero SAML2- SDK.zip.

Una vez la aplicación ha pasado las pruebas pertinentes se recomienda eliminar los siguientes ficheros del WAR que finalmente quedará desplegado: error.jsp, index.jsp, logout.jsp y MyPage.jsp.

2.5 Publicación de aplicaciones para el acceso desde dentro y fuera de la Red Corporativa de la Junta de Andalucía

Si se desea dar de alta una aplicación en SSOWeb que está publicada tanto dentro como fuera de RCJA es necesario configurar en ella el protocolo SAML utilizando la url para acceder desde fuera de RCJA de forma que los metadatos generados expresen esta url.

Una vez hecho esto los responsables de la aplicación integrada deberán solicitar a su Servicio de Producción (o similar) que los accesos internos (realizados desde dentro de RCJA) se atiendan siempre como Proxy Inverso sin realizar redirecciones al dominio interno.

3 Aplicación de ejemplo distribuida ya configurada

Para facilitar la integración se distribuye una aplicación de pruebas ya configurada y operativa contra el entorno de integración del SSOWeb. Puede descargar el WAR de la url:

https://redprofesional.juntadeandalucia.es/file/view/21092216/springsamlintegrationexamplewar

Para que el WAR funcione debe añadir la siguiente línea al fichero /etc/hosts de la máquina en que vaya a desplegarlo:

127.0.0.1 samlintegration.sandetel.int

Una vez añadida la línea en el fichero /etc/hosts y desplegado el war en un servidor de aplicaciones puede probar la autenticación contra el SSOWeb accediendo en un navegador web a la url:

http://samlintegration.sandetel.int:8080/SpringSAMLIntegrationExample/MyLogin.jsp

y pulsar en el enlace "Autenticación contra SSOWeb en el entorno de integración".