Servicio de WebSSO

Manual de integración de aplicaciones PHP con openAM

Versión: 0104

v104

HOJA DE CONTROL

Organismo	Sandetel		
Proyecto	Single Sign-On Web		
Entregable	Manual de integración		
Autor	Francisco Rodríguez Corredor		
Aprobado por		**Fecha aprobación**	15/02/2018
		Nº total de páginas	9

REGISTRO DE CAMBIOS

Versión	Causa del cambio	Responsable del cambio	Fecha del cambio
100	Versión inicial	Francisco Rodríguez Corredor	20/05/2015
101	Registro de bug al utilizar PHP 5.2	Francisco Rodríguez Corredor	02/07/2015
102	Simplificación del proceso de integración	Francisco Rodríguez Corredor	06/07/2015
103	Reordenación de contenidos	Francisco Rodríguez Corredor	29/03/2016
104	Revisión	UPSH	17/02/2020

CONTROL DE DISTRIBUCIÓN

Nombre y apellidos

ÍNDICE

1 OBJETIVO

El objetivo del presente documento es servir de guía para la integración de aplicaciones PHP que quieran hacer uso de las funcionalidades disponibles en el sistema de Single Sign On Web openAM, en adelante SSOWeb.

1.1 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, auditoría 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 DE APLICACIONES PHP

2.1 Prerequisitos

Es necesario tener instalado el servidor Apache2, con el módulo de PHP5 instalado y configurado y con un certificado correctamente configurado e instalado para acceder al mismo por https.

Para que funcione el inicio de sesión automático cuando el usuario acceda a la aplicación integrada si ya tiene iniciada sesión de forma previa en el SSOWeb es necesario que la aplicación que desea integrar esté el mismo subdominio que el SSOWEB y que es *.juntadeandalucia.es

2.2 Procedimiento de configuración e integración

El proceso de integración de una aplicación PHP con el SSOWEB se compone de los siguientes pasos:

- Descarga e instalación del software SimpleSAMLPHP preconfigurado para el SSOWEB de la Junta de Andalucía. Este paquete se encuentra disponible en la sección de ficheros del grupo 'Single Sign-On' de la Red Profesional:

  https://redprofesional.juntadeandalucia.es/groups/profile/192713/single-sign-on

- Registro de nuestra aplicación en el entorno operativo del SSOWEB que se desea utilizar en la integración. Esta tarea le corresponde al administrador funcional del SSOWEB y se solicita mediante un ticket NAOS tal y como se detalla más adelante.
- Modificación de la aplicación a integrar para invocar los métodos correspondientes proporcionados por SimpleSamlPHP.

2.2.1 Configuración básica SimpleSAMLPHP

Una vez descargado el recurso SimpleSAMLPHP preconfigurado para el SSOWEB de la Junta de Andalucía, es necesario realizar los siguientes pasos:

1. Crear el directorio /opt/software/simplesamlphp en la máquina en la que se va a ubicar el servidor de aplicaciones sobre el que se ejecuta la aplicación que se desea integrar. De aquí en adelante a este directorio se le refenciará como $SIMPLESAMLPHP_DIR
2. Otorgar el directorio anteriormente creado permisos de lectura, escritura y ejecución para el usuario que ejecuta el servicio correspondiente al servidor Apache.
3. Descomprimir el paquete SimpleSAMLPHP_JDA.tar.gz en la carpeta anteriormente creada.
4. Si va a utilizar otra ruta del sistema de ficheros a tal efecto, deberá modificar las siguientes propiedades del fichero /$SIMPLESAMLPHP_DIR/config/config.php:
   - certdir
   - loggingdir
   - datadir

5. Abrir una consola del sistema y lanzar el siguiente comando:

   "tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom |dd bs=32 count=1 2>/dev/null;echo"

   Recuperar la salida del comando y cambiar el valor de la propiedad "secretsalt" del fichero /$SIMPLESAMLPHP_DIR/config/config.php por el valor obtenido.

6. Editar también en el fichero /$SIMPLESAMLPHP_DIR/config/config.php la propiedad 'baseurlpath' estableciendo para ella una url de la forma: 'https://<nombre_del_servidor>/simplesaml/'.

7. Editar el fichero /$APACHE_DIR/apache/conf/httpd.conf y añadir el siguiente bloque de texto al final del fichero:

```
<IfModule alias_module>
        Alias /simplesaml/ "/opt/software/simplesamlphp/www/"
            <Directory "/opt/software/simplesamlphp/www">
                AllowOverride None
                Options None
                Order allow,deny
                Allow from all
        </Directory>
</IfModule>
```

   Si ha desplegado SimpleSamlPHP en otro directorio diferente deberá modificar el texto indicado en el punto anterior para adaptarlo con los directorios correctos.

8. Parar y arrancar Apache para que los cambios tomen efecto.

9. Comprobar que el punto de montaje de la aplicación web es correcto:

   - Acceder a https://<nombredelservidor>/simplesaml/
   - Pulsar en "Entrar como administrador". Cuando solicite una contraseña introducir: 123456
   - Si se desea cambiar esta contraseña se puede editar el archivo /$SIMPLESAMLPHP_DIR/config/config.php y cambiar la propiedad "auth.adminpassword" por la contraseña deseada.

10. Pulsar en la pestaña "Configuración" y en el apartado "Verificación de su instalación de PHP" verificar que todo lo marcado como "Necesario" supera la verificación. Lo marcado como "Necesario para LDAP" no es obligatorio.

11. En el apartado "Configuración" también, pulsar sobre el enlace "Sanity check of your simpleSAMLphp setup" y comprobar que se superan todas las comprobaciones.

12. El SimpleSamlPHP que se distribuye con esta guía está preconfigurado con los metadatos necesarios para los entornos de integración, preproducción y producción, por lo tanto Vd sólo tendrá que seleccionar en su integración contra qué entorno del SSOWEB se quiere integrar. Para ello establezca en el fichero /$SIMPLESAMLPHP_DIR/config/authsources.php el parámetro "idp" correspondiente al entorno correcto según lo indicado en la siguiente tabla a su valor correspondiente para la entrada 'default-sp' que comienza en la línea 13 del fichero:

	idp
Integración	https://ssoweb.int.i-administracion.junta-andalucia.es:443/opensso
Preproducción	https://ssoweb.pre.juntadeandalucia.es/opensso
Producción	https://ssoweb.juntadeandalucia.es/opensso

13. Una vez configurado el entorno destino del SSOWEB a utilizar, 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":

    https://naossuite.juntadeandalucia.es/autoservicio/faces/xhtml/incident/newIncident.xhtml?serviceId=74&operationId=43&componenteId=113822&elementoId=359462

    En el ticket creado indique la siguiente información:

- Nombre de la aplicación a integrar.
- Consejería u organismo al que pertenece la aplicación a integrar.
- Datos de contacto del responsable del servicio asociado a la aplicación a integrar: nombre, apellidos, teléfono y correo electrónico.
- Url de metadatos SimpleSamlPHP de la aplicación integrar. Será del tipo https://<nombre_del_servidor>/simplesaml/module.php/saml/sp/metadata.php/default-sp

(*) Si no puede ver este procedimiento en NAOS, solicite permisos para ello utilizando un ticket del tipo:

http://naossuite.juntadeandalucia.es/autoservicio/faces/xhtml/incident/newIncident.xhtml?serviceId=74&operationId=10&componenteId=113822&elementoId=359441

14. Una vez dado de alta su sistema en el SSOWEB correspondiente ya sólo falta que modifique el código de su aplicación para que invoque correctamente los métodos que SimpleSamlPHP le ofrece para la integración utilizando el protocolo SAML2.0. En el siguiente apartado se muestra una integración de ejemplo que debe servirle como referencia de las modificaciones a realizar.

3 Integrando su aplicación con el SSOWeb

Para facilitar la integración de aplicaciones PHP con el SSOWEB se ha generado una librería que permite invocaciones a la lógica del sistema.

Para hacer uso de estas librerías únicamente tiene que realizar los siguientes pasos:

1. Descomprima el recurso SDK.tar.gz distribuido junto con este manual en el mismo directorio en el que tiene la aplicación PHP que desea integrar. Verifique que se ha creado un fichero llamado AppExample.php y una carpeta llamada "SAML" con los siguientes ficheros: auth.php, configuration.php, SamlAuthentication.php y SAMLlib.php

   El fichero AppExample.php es un ejemplo básico de invocación al SSOWeb. Ejecutelo en su servidor de desarrollo a modo de demo y una vez haya finalizado las tareas de desarrollo elimínelo para que no progrese a entornos productivos

2. edite el fichero "SAMLlib.php" contenido en la carpeta "SAML" que acaba de descomprimir y configure correctamente la línea 2 del fichero indicando la ruta completa al fichero *_autoload.php* de su instalación de SimpleSamlPHP

3. edite el fichero configuration.php contenido en la carpeta "SAML" y descomente la línea de corresponda para el entorno contra el que se desea integrar: línea 17 para el entorno de integración, 18 para preproducción y 19 para producción

4. cargue en su aplicación PHP el código de la librería SAMLlib.php incluyendo en la misma la línea "require_once ('./SAML/SAMLlib.php');"

5. invoque a la función "iniciarLoginSSOWeb()" cuando en el flujo de su aplicación desee iniciar el procedimiento de login por SSOWeb. Esta función verificará si el usuario ya tiene iniciada sesión en el SSOWeb. En caso positivo devolverá un array con los atributos de identidad del usuario que le permitirán inicializar la sesión también en la aplicación que se está integrando. Esta función devolverá "null" en caso de que el usuario no tenga iniciada sesión en el SSOWeb.

6. Invoque a la función "realizarLoginSSOWeb()" para inicializar el procedimiento de login mediante el SSOWeb. **Se recomienda que antes de invocar a esta función compruebe utilizando "iniciarLoginSSOWeb()" si el usuario ya tiene iniciada sesión en el SSOWeb para evitarle navegaciones innecesarias**. Intente realizar la implementación siguiendo el orden establecido en la aplicación de prueba "AppExample.php".

7. invoque a la función "obtenerDatosIdentidad()" cuando en el flujo de su aplicación desee obtener los datos de la identidad de usuario

8. Invoque a la función "realizarLogoutSSOWeb()" cuando en el flujo de su aplicación desee cerrar la sesión en el SSOWeb

Si tiene dudas sobre la implementación del mecanismo de SSOWeb consulte la página de ejemplo AppExample.php

4 Problemas conocidos

Mensaje de error:

> *"Parse error: syntax error, unexpected T_FUNCTION in /simplesamlphp/modules/core/lib/Auth/Process/GenerateGroups.php on line 139"*

Si está realizando la instalación en una máquina con versión 5.2 de PHP y le aparece el mensaje anterior consulte el siguiente enlace para saber cómo solucionarlo:

http://stackoverflow.com/questions/20402145/simplesamlphp-unexpected-t-function-in-generategroups-php