Servicio Web de Programación Dinámica:
Federación de aplicaciones PHP (Autenticación con credenciales UGR)

El Servicio de autenticación de usuarios UGR está dirigido a aquellos portales web UGR , alojados en wpd.ugr.es, que necesiten comprobar y controlar el acceso de los usuarios a los módulos o informaciones que publican y no desean mantener una gestión local de usuario/password en el propio portal.

Los desarrolladores de estas webs institucionales, o autorizadas, pueden autenticar a los usuarios UGR con sus credenciales de correo electrónico, sin necesidad de mantener/programar un sistema alternativo de usuarios y claves locales. De esta forma se aseguran que el usuario autenticado pertenece a la comunidad universitaria y que la dirección electrónica del usuario se corresponde con quien dice ser.

Incorporando una sencilla programación en la aplicación, cuando el portal solicite al usuario su autenticación, automáticamente se le redirigirá a los Servidores de Identidad institucionales, donde se pedirá su dirección de correo electrónico y clave, y devolverá al portal 'federado' si el usuario ha sido realmente reconocido y, en una variable, la dirección electrónica del mismo.

Aquellos portales identificados como “Federados con el Servicio de Identidad de UGR” pueden asegurar a sus usuarios que la autenticación es totalmente segura siendo imposible para ellos capturar o conocer el password del mismo; la autenticación se produce siempre, por canales cifrados, en los proveedores de identidad (IDPs) del CSIRC y nunca en el propio portal web.

Centro de Servicios de Informática y Redes de Comunicaciones
Edificio Mecenas * Campus Fuentenueva * 18071 Granada
Telf. 958 241010 * Fax 958 244221 * Web http://csirc.ugr.es * eMail csirc@ugr

A continuación mostramos un ejemplo de federación de una aplicación PHP sencilla:

1. Descargue y descomprima el fichero, ***Ejemplo federación***, que encontrará en la web junto con este tutorial.
   Si lo examina, podrá observar que el directorio federación está compuesto por cuatro archivos:

   - **config.php :** fichero de configuración.
     En él se define dónde se encuentra el archivo que carga las librerías de simpleSAMLphp, se cargan dichas librerías, se define la URL base de nuestra aplicación y el SP que se utilizará como fuente de autenticación.

   - **login.php:** fichero de inicio de sesión.
     Redirige al usuario para que inicie el login en el Idp y una vez autenticado vuelve a la pagina principal.

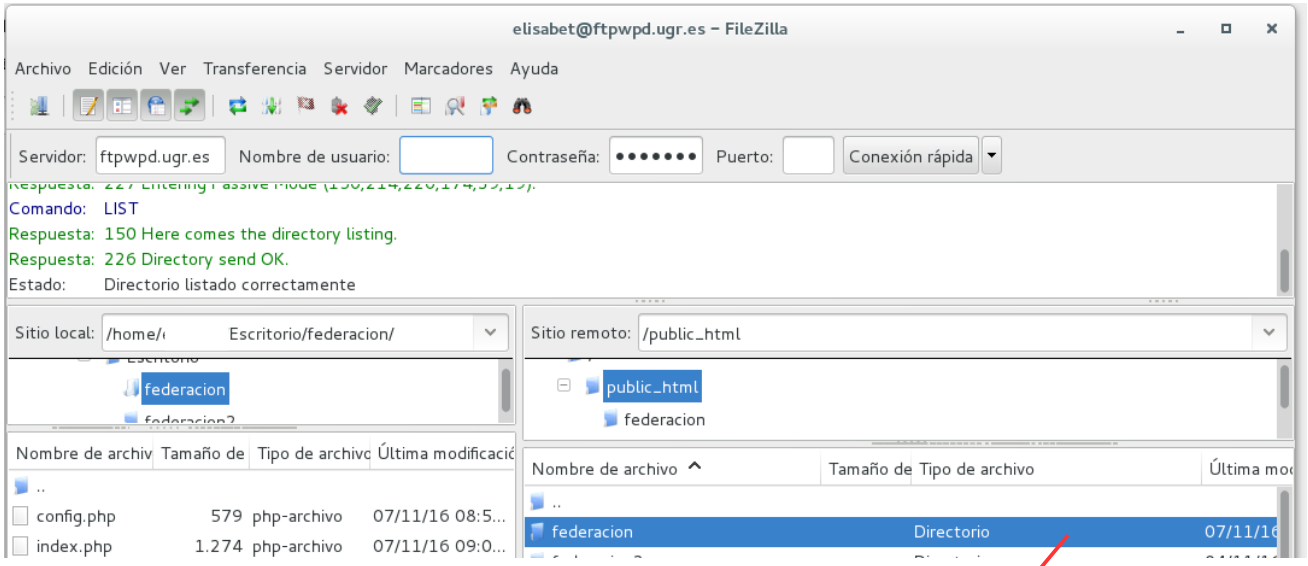
   - **logout.php:** fichero de cierre de sesión.
     Comprueba si el usuario está autenticado en el sistema y fuerza el deslogueo en el Idp si es que lo está. Una vez deslogueado redirige al usuario a la página principal.

   - **index.php:** Página principal de nuestra aplicación.
     El usuario aún no está identificado, se le ofrece un enlace para hacerlo, una vez autenticado se muestra su email y se le facilita el enlace para cierre de sesión.

2. Suba el directorio federación a su ***public_html.***
   Puede hacerlo utilizando un cliente FTP, nosotros hemos usado Filezilla (***https://filezilla-project.org/download.php?type=client***). Conéctese con su usuario y password a ***ftpwpd.ugr.es*** , suba el directorio y compruebe que todos los archivos tienen permisos 640 haciendo clic derecho sobre el archivo y seleccione ***Permisos de archivo...***(vea imagen1)

3. Puede probar la funcionalidad del ejemplo desde su navegador accediendo a wpd.ugr.es/~usuario/federación/index.php

4. Modifique el archivo index.php para que se adapte a sus necesidades o adapte el código propuesto e inclúyalo en su archivo index.php que ya debería tener en el directorio public_html.



IMPORTANTE:

Puede modificar todos los ficheros para adaptarlos a sus necesidades salvo ***config.php*** que contiene la configuración de las librerías simpleSAML2

¿Hay diferencia entre autenticación y autorización?

Si, el proceso de **autenticación** permite asegurar que un usuario de un sitio web es auténtico o quien dice ser, mientras que el de **autorización** permite a los usuarios que reúnen ciertas características o que tienen permiso, a acceder a recursos protegidos.

Llegados a este punto del tutorial, si incorpora el código del ejemplo anterior y lo adapta a su aplicación, su web será capaz de comprobar que los usuarios que se autentican en ella son miembros de la comunidad universitaria, pero si lo que quiere es mostrar contenido de su web en función del tipo de usuario, perfiles , etc. deberá implementar su propio código de **autorización.**

Al generar su código para autorizar no olvide que se encuentra en un entorno compartido multiusuario, en el que las variables de sesión son accesibles por todos los usuarios. Es por ello, que le recomendamos el uso de ***cookies***.

A continuación le mostramos un ejemplo sencillo de uso de cookies:

```
<?php
  // Definimos la ruta y duración de la cookie.
  define("COOKIE_PATH", "wpd.ugr.es/~miusuario");
  define("COOKIE_EXPIRATION", time()+60*60*24*30); // 1 mes

  // Proceso de Autenticación
  require_once('/var/simplesamlphp/lib/_autoload.php');
  $as = new SimpleSAML_Auth_Simple('default-sp');
  $as->requireAuth();
  if ($as->isAuthenticated())
  {
    $attributes = $as->getAttributes();
    $emailuser = $attributes['mail'][0];

    //Creamos la cookie usuario con los valores definidos anteriormente.
    setcookie("usuario", $emailuser, COOKIE_EXPIRATION, COOKIE_PATH);

   //Autorizacion (basada en código) con 2 tipos de usuarios
    $moderadores=array('usuario1@ugr.es');
    $administradores=array('usuario2@ugr.es');
```

```
    //comprobar si es un administrador
      if (in_array($emailuser, $administradores)){
         setcookie("tipo", 'administrador', COOKIE_EXPIRATION, COOKIE_PATH);
      }elseif (in_array($emailuser, $moderadores))
    //comprobar si es un moderador
      {
            setcookie("tipo", 'moderador', COOKIE_EXPIRATION, COOKIE_PATH);
      }else{
    // es otro tipo de usuario
            setcookie("tipo", 'otro', COOKIE_EXPIRATION, COOKIE_PATH);
      }
  }else{
      echo("No está autorizado");
      exit();
  }

…

//Código de su web que muestra información dependiendo del tipo de usuario
que se ha autenticado en ella

…

?>
```

Si prefiere usar **sesiones**, es muy importante que haga uso de la función **session_name** para establecer su nombre de sesión. Ejemplo:

```
<?php
  // Proceso de Autenticación
  require_once('/var/simplesamlphp/lib/_autoload.php');

  $as = new SimpleSAML_Auth_Simple('default-sp');
  $as->requireAuth();

  if ($as->isAuthenticated())
  {
    $attributes = $as->getAttributes();
    $emailuser = $attributes['mail'][0];

    session_name("wpd_miusuario");
    $_SESSION['usuario'] = $emailuser;

    //Autorizacion (basada en código) con 2 tipos de usuarios
    $moderadores=array('usuario1@ugr.es');
    $administradores=array('usuario2@ugr.es');

    //comprobar si es un administrador
     if (in_array($emailuser, $administradores)){
           $_SESSION['tipo'] = 'administrador';
     //comprobar si es un moderador
     }elseif (in_array($emailuser, $moderadores)){
          $_SESSION['tipo'] = 'moderador';
     }else{
          unset($_SESSION['tipo']);
     }

   }else{
        echo("No está autorizado");
        exit();
   }
```

```
…

//Código de su web que muestra información dependiendo del tipo de usuario
que se ha autenticado en ella

…

?>
```