SimpleSAMLphp (IdP de referencia)

Introducción

Esta guía ofrece los pasos a seguir para realizar una instalación desde cero de SimpleSAMLphp con el objetivo de disponer de un Proveedor de Identidad con el que conectarse a la federación SIR2 ofrecida por el Servicio de Identidad de RedIRIS. Para ello se ha creado un módulo para SimpleSAMLphp que a través de unos sencillos pasos prepara y pre-configura dicho software.

La integración con distintas fuentes de datos en la organización (directorios LDAP, bases de datos relacionales, o sistemas de single-sign-on como CAS o ADFS) queda del lado de la organización, sin embargo en la sección "recetas de integración" de esta guía, se irán poniendo ejemplos que pueden ser usados por las organizaciones realizando un despliegue.

Este documento no cubre los aspectos de una actualización de un despliegue ya realizado de SimpleSAMLphp, para lo cual recomendamos la lectura de la documentación oficial del software al respecto. Resumiendo el proceso de actualización, ésta pasaría por realizar una copia de seguridad de la versión previa de producción, la instalación de la nueva versión, y la sustitución de ficheros de configuración, plantillas y metadatos.

Esta guía ha sido desarrollada sobre la versión 1.17.2 de SimpleSAMLphp. Más adelante se describe cómo descargar e instalar este software ejecutando un sencillo comando.

Pre-requisitos del IdP de referencia

Para poder ejecutar el módulo que instala y realiza una configuración base de SimpleSAMLphp para conectarse al SIR, será necesario que esté disponible a través de un servidor web, en el ejemplo se utiliza un servidor Apache.

Con carácter general, los pre-requisitos de SimpleSAMLphp están listados en la siguiente URL:

https://simplesamlphp.org/docs/stable/simplesamlphp-install#section_3

Resumimos en la siguiente lista los prerequisitos mínimos que deberemos tener en el servidor donde se va a desplegar SimpleSAMLphp:

- Servidor web con capacidad de ejecutar PHP
- PHP versión 5.5.0 o superior
- Módulos PHP: `date`, `dom`, `hash`, `libxml`, `openssl`, `pcre`, `SPL`, `zlib`, `mbstring`, `json`
- El paquete del sistema de control de versiones git
- Existen otros módulos opcionales que deberán instalarse en el caso de querer utilizar determinada funcionalidad:
  - Módulo LDAP de PHP, si se quiere utilizar LDAP para la autenticación o la atribución
  - Módulo PDO de PHP, si se quiere utilizar una base de datos para la autenticación o la atribución. Además, será necesario instalar algún driver específico de PDO: mysql, pgsql, etc.
  - Módulo Memcache de PHP, si se va a utilizar Memcache para gestionar las sesiones PHP

NOTA: Se ha descrito una instalación en entorno Windows + Apache + PHP, si bien es preferible y recomendamos su instalación en un entorno Linux reciente.

IMPORTANTE: se recomienda que la instalación del IdP de referencia sea efectuada por una persona con experiencia en el despliegue de servidores web (Apache como servidor web de referencia) y aplicaciones PHP.

Instalador del IdP de referencia

Para instalar el paquete completo que incluye:

- SimpleSAMLphp
- Módulo IdP Installer

- Módulo Updater
- Tema Sir2Skin

Debemos de utilizar la nueva herramienta de instalación, que utiliza Composer como base para la gestión de paquetes. Se pueden consultar los detalles aquí.

Modificación de la URL base de simpleSAMLphp

Al ejecutar el instalador, se ha debido de configurar de manera satisfactoria todos los ficheros de configuración del simplesamlphp, de todos modos debemos cerciorarnos, para poder continuar con la instalación, que la directiva “baseurlpath” ubicada en el fichero de configuración /var/www/html /simplesamlphp/config/config.php se encuentre como sigue:

```
'baseurlpath' => '/',
'certdir' => 'cert/',
'loggingdir' => 'log/',
'datadir' => 'data/',
...
```

En la línea `24: '/'`, es importante que se dejen las comillas simples puesto que si no es así se producirá un error al ejecutar SimpleSAMLphp. En caso de que la máquina que sirve el contenido se encuentre tras un balanceador, es posible poner en este campo la dirección completa (por ejemplo: `https://sso.rediris.es:443`).

NOTA IMPORTANTE: En este ejemplo se asume que la instalación se ha realizado en el raíz del servidor web, en caso de que se realiza sobre otra localización, en `baseurlpath` debería ponerse la ruta web, por ejemplo, **`'baseurlpath' => '/login',`**.

Configuración de Apache

En el siguiente ejemplo se asume que SimpleSAMLphp está instalado en la localización que por defecto espera el software: `/var/www/html /simplesamlphp`

Del mismo modo se asume que usted ya dispone de un servidor web Apache en su sistema y que está configurado para responder peticiones HTTP seguras.

El único subdirectorio de SimpleSAMLphp al que debe tener acceso el servidor web es el directorio www/. Existen varias opciones para servir SimpleSAMLphp en función de como esté estructurado el servidor web apache. La configuración aquí utilizada es la recomendada por los desarrolladores de SimpleSAMLphp, donde se sirve dicho software a través de un host virtual de Apache. Busque el fichero de configuración de Apache para los “virtual hosts” donde quiera ejecutar SimpleSAMLphp. La configuración del virtual host, deberá ser parecida a la siguiente:

```
<VirtualHost *:443>
        ServerName nombreDelServidor
        DocumentRoot /var/www/html/simplesamlphp/www
        # Configuración de servidor seguro
        ...
        # Fin configuración de servidor seguro
        Alias / /var/www/html/simplesamlphp/www/
        <Directory /var/www/html/simplesamlphp/www>
                Options -Indexes +FollowSymLinks
                AllowOverride None
                Order deny,allow
                Allow from all
        </Directory>
        <Location />
                Options FollowSymLinks
                AllowOverride None
                Order deny,allow
                Allow from all
        </Location>
</VirtualHost>
```

Tras realizar la modificación del fichero de configuración de Apache debe reiniciar el servidor para que los cambios surtan efecto.
Una vez reiniciado el servidor web Apache puede acceder al interfaz web de instalación y configuración de SimpleSAMLphp en una URL con el siguiente formato: `https://miservidorweb/module.php/idpinstaller/`.

Seguimiento del proceso de instalación

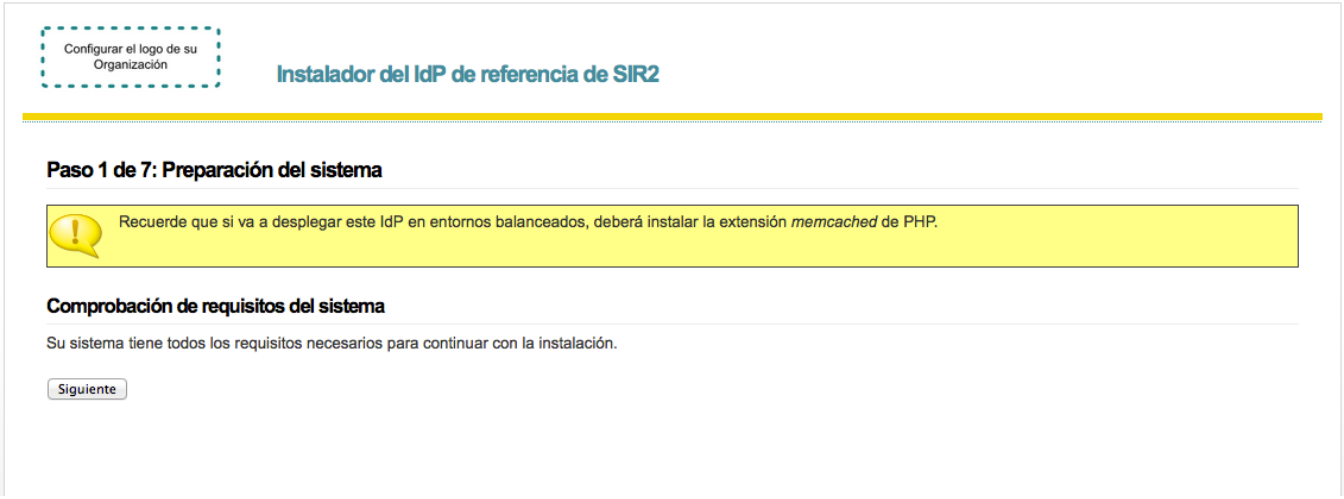
El instalador de conexión con SIR está compuesto por 8 pasos que deberán seguirse para completar el proceso.

Paso 1: Preparación del sistema

El primer paso es comprobar si se cumplen todos los requisitos de sistema para proceder con la instalación.
Si alguno de los requisitos necesarios para proceder con la instalación no se cumpliese, aparecerá en este paso un mensaje de error con una lista de los elementos necesarios para poder continuar, en este caso será necesario proceder a la instalación del elemento requerido en el sistema.

También podría ser necesaria la modificación de los permisos de algunos ficheros o directorios de los que hará uso la herramienta de instalación, en caso de que no se hayan ajustado los permisos, tal y como se indica en el epígrafe sobre desempaquetado de SimpleSAMLphp. En dicho caso se proporcionará al usuario la información necesaria para continuar con el proceso.

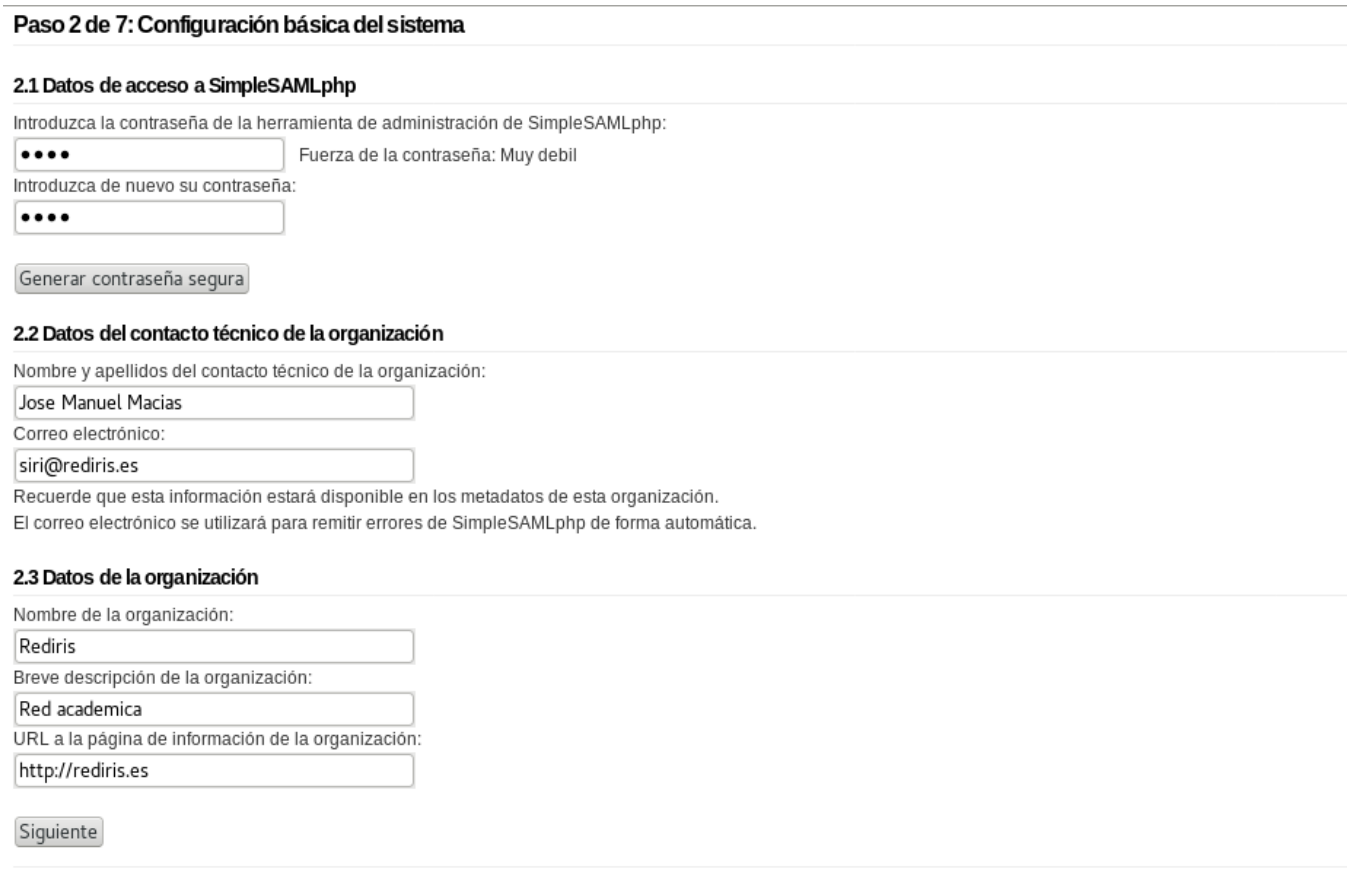
Si todo esta configurado correctamente, tendremos una pantalla como la que sigue:



Paso 2: Configuración básica del sistema

Configuración de datos de acceso a la herramienta SimpleSAMLphp y de la organización que gestionará el sistema.

- **Contraseña de la herramienta de administración**: esta contraseña es la que se asocia al administrador en la herramienta visual de SimpleSAMLphp.
- **Nombre y apellidos del contacto técnico**: datos de la persona técnica responsable del SimpleSAMLphp que se está desplegando. Estos datos serán publicados en los metadatos como Proveedor de Identidad SAML 2.
- **Correo electrónico**: correo electrónico de dicho contacto técnico. Este correo se utilizará tanto en los metadatos como para la recepción de errores que SimpleSAMLphp envíe en el caso de que se produzcan.



Tras continuar y comprobar que los datos introducidos son los correctos, se hace una comprobación de la zona horaria, si esta es incorrecta, se deberá comprobar la configuración del parámetro timezone en el fichero php.ini y también modificar el timezone en el fichero de configuración de simpleSAMLphp. config.php, tal y como se indica aquí

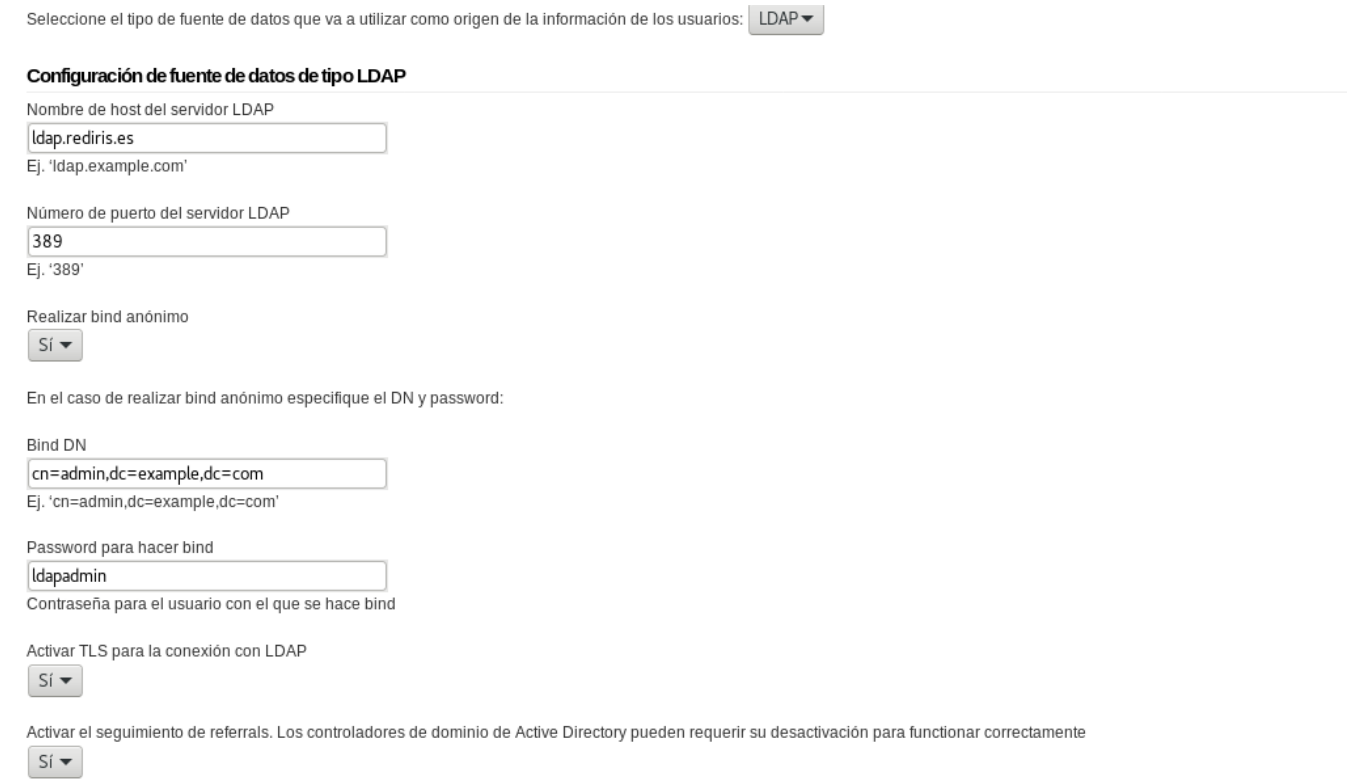
Paso 3: Configuración de fuente de datos

En este paso se configura la fuente de datos que se quiere utilizar para autenticar y realizar la atribución. Los tipos de fuentes de datos que estarán disponibles para ser seleccionados serán LDAP o bien PDO en el caso de querer utilizar una base de datos.

En caso de no tener establecidos correctamente los permisos los ficheros y directorios, la herramienta proporcionará al usuario la información necesaria para continuar con el proceso.

Tipo de fuente de datos LDAP

- **Nombre de host del servidor LDAP**: FQDN del servidor LDAP en el que se encuentran las cuentas de usuario de la organización. Por ejemplo: ldap.rediris.es
- **Número de puerto del servidor LDAP**: Puerto por el que se accede al servidor LDAP. Por defecto es el 389, aunque puede variar según la configuración.
- **Realizar bind anónimo**"Si" en caso de querer permitir el bind anónimo para acceder al servidor.
- **Bind DN**: En caso de que bind anónimo sea "Si", el DN a utilizar para realizar el bind anónimo.
- **Password para hacer bind**: En caso de que bind anónimo sea "Si", la contraseña para realizar el bind anónimo.
- **TLS**: “Sí” en el caso de querer realizar una conexión segura con el servidor LDAP, “No” en caso contrario
- **Referral**: activación del uso de referrals en el LDAP. Puede ser necesario desactivarla en el caso de utilizar un Directorio Activo de Microsoft.



NOTA: Para terminar de configurar correctamente la conexión con el LDAP, tendremos que hacer algunas otras modificaciones en el fichero simpleSAMLphp/config/authsources.php. Puede encontrar ejemplos de configuración de este fichero en la "Receta para conexión del IdP con fuentes de datos LDAP".

Tipo de fuente de datos PDO

Dentro de las fuentes de datos tipo PDO se incluyen las Bases de Datos y las fuentes SQL (MySQL, Postgresql, Oracle, etc).

- **DSN de conexión de la base de datos**: Éste es el nombre de la fuente que se usará para realizar la conexión. Deberá tener el siguiente formato: '<driver>:host=<host>;port=<port>;dbname=<dbname>;unix_socket=<socket>'

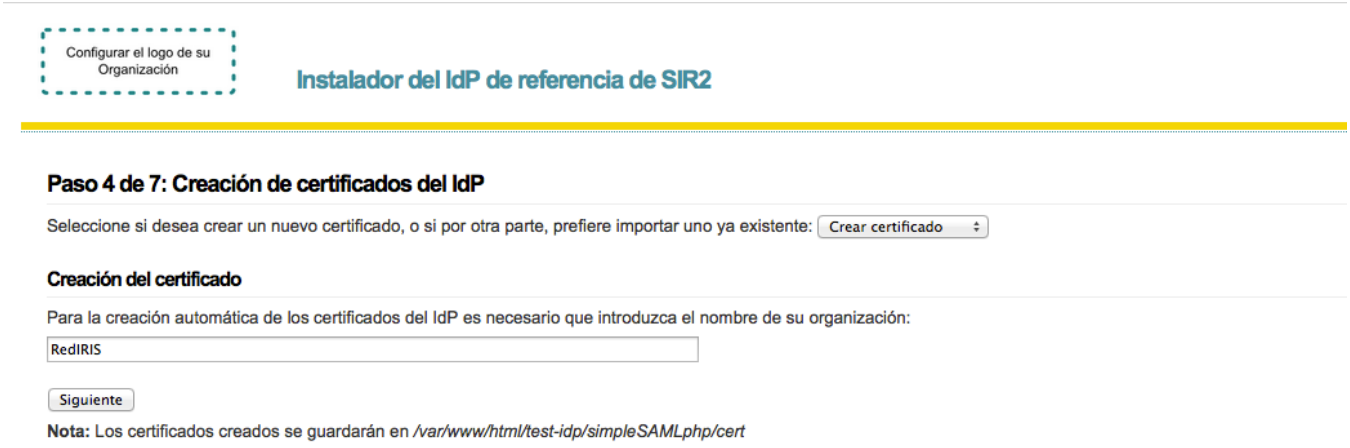
Donde '<driver>' será el conector de la fuente (p.e. 'mysql'), '<host>' será el nombre que identifique al anfitrión (p.e. 'localhost'), '<port>' será el número del puerto de conexión, '<dbname>' el nombre de la base de datos a conectar, y '<socket>' la ruta del socket a utilizar (si procede).

- **Nombre de usuario**: Nombre del usuario que figura como administrador de la fuente de datos.
- **Contraseña**: Contraseña del usuario que figura como administrador de la fuente de datos. Este campo podría estar vacío si la fuente de datos no estuviera protegida por contraseña.

NOTA: Podemos ver ejemplos de configuración de fuentes PDO en la sección de recetas de esta guía.

Paso 4: Creación de certificados del IdP y configuración del protocolo SAML 2.0

Este paso permite crear los certificados digitales necesarios para la instalación, o bien la utilización de uno ya creado.
El instalador posee la capacidad de crear automáticamente los certificados del proveedor de identidad. Para ello es necesario introducir como dato el nombre de la organización a la que hará referencia dicho certificado.

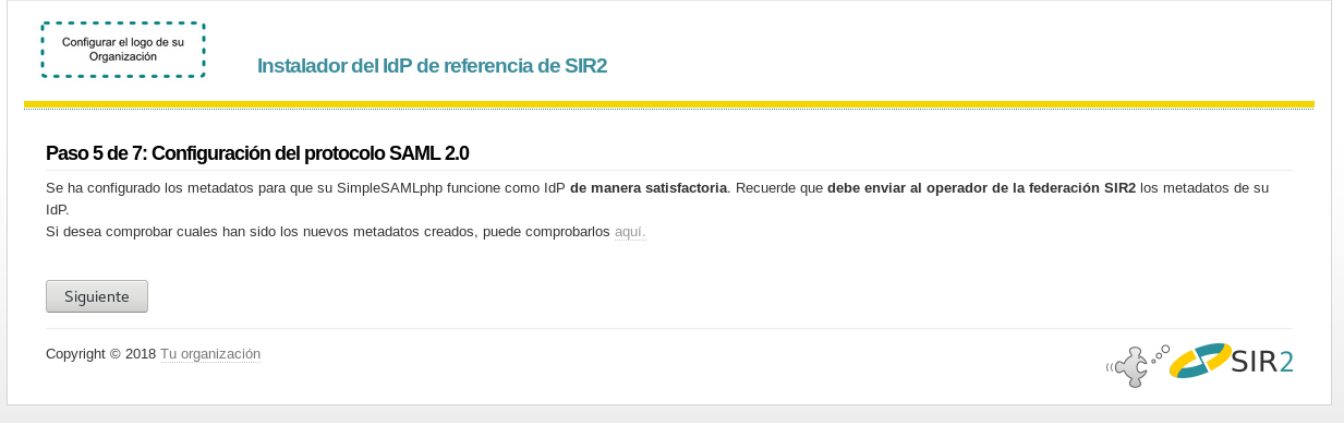


Si desea modificar el script de creación de certificados digitales, puede encontrar dicho script bajo la ruta `modules/idp_installer/lib/makeCert.sh` de su instalación.
Como segunda opción, si ya se posee un certificado y una clave privada para el proveedor de identidad pueden introducirse manualmente. El certificado y la clave privada deben ser válidos, y coincidir.

Si no existe el directorio `'simplesamlphp/cert'` aparecerá un mensaje de error junto con unas indicaciones que le permitirán resolverlo, y otorgarle los permisos necesarios al directorio.
También se realiza en este paso la configuración como Proveedor de Identidad SAML 2.0 y la comprobación de los metadatos para el correcto funcionamiento de SimpleSAMLphp.

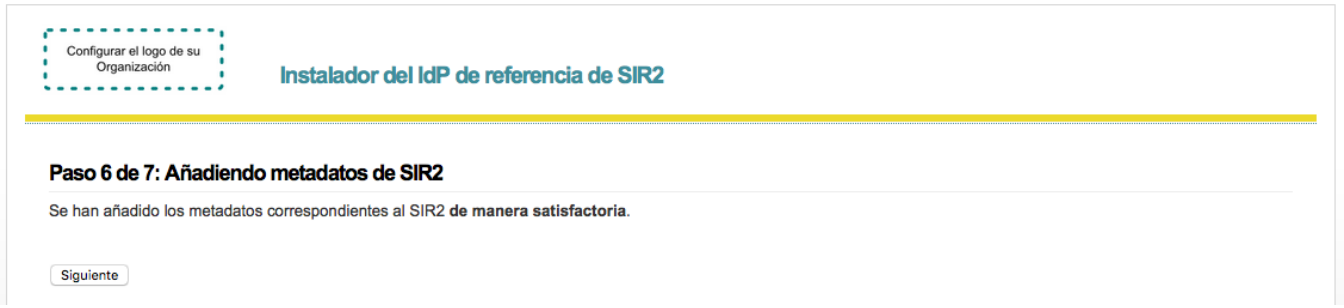
Paso 5: Confirmación de la configuración del Proveedor de Identidad SAML 2.0

En este se nos informa si se los metadatos de nuestro proveedor de identidad se han generado correctamente, y podremos comprobarlos utilizando el enlace que nos muestra la herramienta.



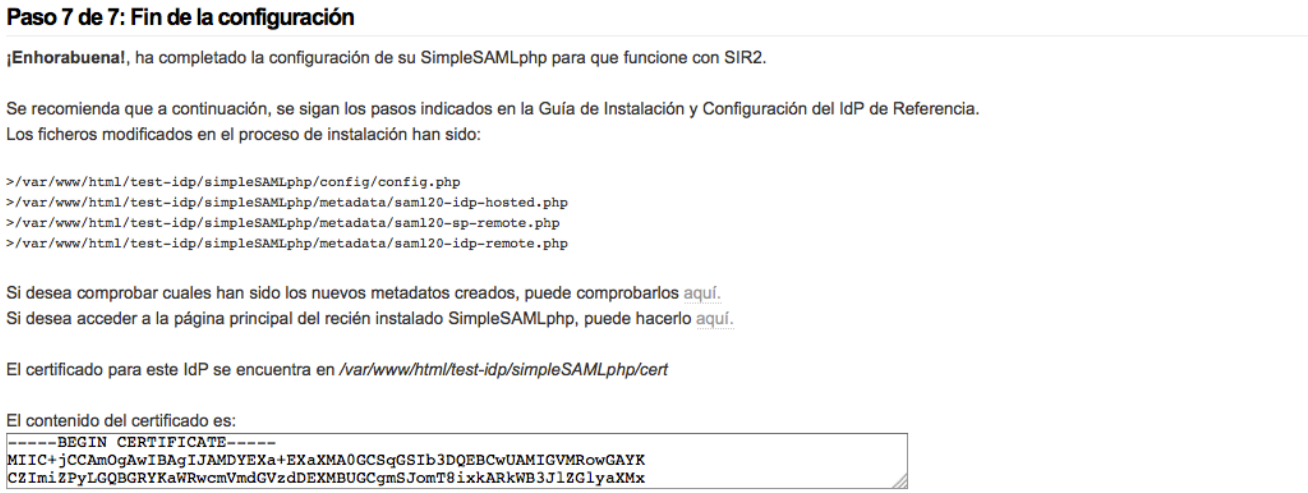
Paso 6: Añadiendo metadatos del SIR

Se realiza la comprobación de la correcta incorporación de los metadatos del SIR en el SimpleSAMLphp.



Paso 7: Fin de la configuración

Este paso muestra un mensaje de confirmación tras la finalización del proceso de instalación, junto con una recomendación referente al cambio de permisos de los ficheros y directorios de SimpleSAMLphp.
Adicionalmente se muestra también el certificado del IdP junto con la ruta en la que se ha guardado.



Configuración de metadatos de la federación

La federación SIR2 utiliza un único conjunto de metadatos SAML para el hub, independientemente de que el IdP esté disponible a través del entorno de pruebas o el de producción.

Si no se ha utilizado el instalador del IdP de referencia, es necesario incorporar los metadatos del hub de la federación en nuestro IdP. Estos metadatos serían los correspondientes a un único proveedor de servicios (el hub de SIR2), con independencia también de que el proveedor de identidad quiera añadir otros proveedores de servicio adicionales.

Para incorporar manualmente los metadatos de la federación, hay que ir a la página de metadatos de la federación, y descargar el conjunto de metadatos XML del hub.

En el caso del IdP de referencia, los metadatos han de ser convertidos al formato de metadatos que acepta el proveedor de identidad, para ello, podemos utilizar la propia **herramienta de análisis de metadatos XML** de nuestro IdP, que se puede localizar a través de un enlace que encontraremos en la sección «Federación» de nuestro SimpleSAMLphp.

La herramienta tiene este aspecto:

Configurar el logo de su Organización

Analizar metadatos

Analizar metadatos

Metadatos XML

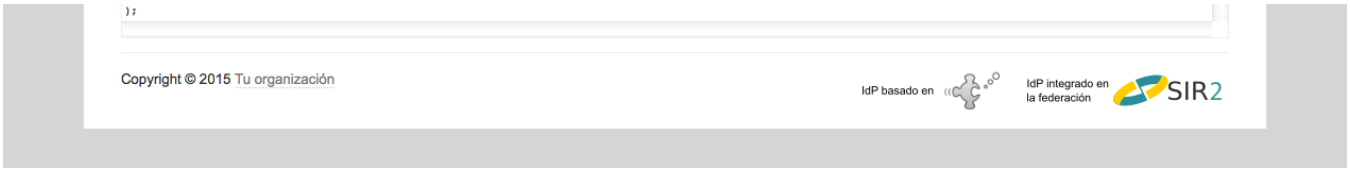
```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="https://sir2-test.rediris.es/metadata/sml/saml2/">
    <md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>

<ds:X509Certificate>MIICsDCCAhmgAwIBAgIJALWPNc3PeGuVMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTAwNjA2MTUxMzMzWhcNMjAwNjA1MTUxMzMzWjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCvvvT7zY9D1DQCsYm8b6I/QEXyX1yzGuciD4HCZ7pYCZ2ehmpXWYCRLaNx7ZM1
YXEWuuo9F4Io7sqa0D+aDAvZsHRn71zoZgzmvHt2D0OPl35aK3BQZSKqMvfjXb2q
Gl3jNvFZPwHxwLaQwyM7I64ZIa86TKK/NYL+vr9+Wz7/lQIDAQABo4GnMIGkMB0G
AlUdDgQWBBRSlnWPNzWG/nK2OwHnI26EkY7IjTBlBgNVHSMEbjBsgBRSlnWPNzWG
/nK2OwHnI26EkY7IjaFJpEcwRTELMAkGAlUEBhMCQVUxEzARBgNVBAgTClNvbWUt
```

Analizar

Metadatos convertidos

saml20-sp-remote

```
$metadata['https://sir2-test.rediris.es/metadata/sml/saml2/'] = array (
  'entityid' => 'https://sir2-test.rediris.es/metadata/sml/saml2/',
  'contacts' =>
  array (
  ),
  'metadata-set' => 'saml20-sp-remote',
  'AssertionConsumerService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
      'Location' => 'https://sir2-test.rediris.es/SAML2/sml_sp_acs.php',
      'index' => 0,
    ),
  ),
  'SingleLogoutService' =>
  array (
  ),
  'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',
  'keys' =>
  array (
    0 =>
    array (
      'encryption' => false,
      'signing' => true,
      'type' => 'X509Certificate',
      'X509Certificate' => 'MIICsDCCAhmgAwIBAgIJALWPNc3PeGuVMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTAwNjA2MTUxMzMzWhcNMjAwNjA1MTUxMzMzWjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCvvvT7zY9D1DQCsYm8b6I/QEXyX1yzGuciD4HCZ7pYCZ2ehmpXWYCRLaNx7ZM1
YXEWuuo9F4Io7sqa0D+aDAvZsHRn71zoZgzmvHt2D0OPl35aK3BQZSKqMvfjXb2q
Gl3jNvFZPwHxwLaQwyM7I64ZIa86TKK/NYL+vr9+Wz7/lQIDAQABo4GnMIGkMB0G
AlUdDgQWBBRSlnWPNzWG/nK2OwHnI26EkY7IjTBlBgNVHSMEbjBsgBRSlnWPNzWG
/nK2OwHnI26EkY7IjaFJpEcwRTELMAkGAlUEBhMCQVUxEzARBgNVBAgTClNvbWUt
U3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZIIJALWPNc3P
eGuVMAwGAlUdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEAgy8OLlAWP2OFcb7q
pXKP5ipXh7863/Z9twPKCnOsKhaZv7kghQDOibEg8W+wbY0fI3dZOskMYJMLbK9o
LYImu/4yALxb/g4UUmzQV4jgzqn6SjFiFSH/fXj9sJtbguNGfamrmkvbwZWDWag2
eC3PAvY6ooljFJvlyRLhksFe7Pg=
',
    ),
    1 =>
    array (
      'encryption' => true,
      'signing' => false,
      'type' => 'X509Certificate',
      'X509Certificate' => 'MIICsDCCAhmgAwIBAgIJALWPNc3PeGuVMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTAwNjA2MTUxMzMzWhcNMjAwNjA1MTUxMzMzWjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCvvvT7zY9D1DQCsYm8b6I/QEXyX1yzGuciD4HCZ7pYCZ2ehmpXWYCRLaNx7ZM1
YXEWuuo9F4Io7sqa0D+aDAvZsHRn71zoZgzmvHt2D0OPl35aK3BQZSKqMvfjXb2q
Gl3jNvFZPwHxwLaQwyM7I64ZIa86TKK/NYL+vr9+Wz7/lQIDAQABo4GnMIGkMB0G
AlUdDgQWBBRSlnWPNzWG/nK2OwHnI26EkY7IjTBlBgNVHSMEbjBsgBRSlnWPNzWG
/nK2OwHnI26EkY7IjaFJpEcwRTELMAkGAlUEBhMCQVUxEzARBgNVBAgTClNvbWUt
U3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZIIJALWPNc3P
eGuVMAwGAlUdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEAgy8OLlAWP2OFcb7q
pXKP5ipXh7863/Z9twPKCnOsKhaZv7kghQDOibEg8W+wbY0fI3dZOskMYJMLbK9o
LYImu/4yALxb/g4UUmzQV4jgzqn6SjFiFSH/fXj9sJtbguNGfamrmkvbwZWDWag2
eC3PAvY6ooljFJvlyRLhksFe7Pg=
',
    ),
  ),
```



El array asociativo resultante, hay que añadirlo al fichero `saml20-sp-remote.php` que encontraremos en el directorio `metadata/` de nuestro IdP.

Pautas para la instalación de un servidor web seguro

Para formar parte de la federación SIR2 es obigatorio que la URL del IdP esté bajo el protocolo seguro HTTPS. Veamos los pasos y requerimientos necesarios

En primer lugar, debemos de tener instalado el paquete openssl en el servidor.

Una vez instalado openssl, procederemos a la obtención y configuración del certificado. Los certificados son expedidos por Autoridades Certificadoras, por lo que deberemos contactar con alguna de ellas para obtener el certificado. Los certificados seguros tienen un coste, pero **todas las instituciones pertenecientes a la federación pueden obtener el certificado gratuitamente haciendo uso del servicio TCS (https://www.rediris.es/tcs/doc/). Por tanto, recomendamos el uso de este servicio**, aunque se puede obtener de forma independiente asumiendo el coste correspondiente.

Para comenzar, hay que asegurarse de estar dado de alta en el servicio. En caso de no estarlo, hay que seguir los siguientes pasos: https://www.rediris.es/tcs/alta/

Una vez datos de alta en el servicio, obtendremos acceso a https://www.digicert.com/account/login.php. Esta será nuestra Autoridad Certificadora. Desde aqui podremos solicitar el certificado siguiendo los siguientes pasos:

- En primer lugar es necesario generar una clave privada y una Clave de Solicitud de Certificado (CSR). Para ello haremos uso de openssl:

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

- Posteriormente enviaremos la Clave de Solicitud de Certificado (server.csr) a nuestra Autoridad Certificadora mediante su plataforma web.
- Recibiremos por email el certificado de nuestro dominio junto con el certificado de la Autoridad Certificadora.
- Ahora disponemos de los tres ficheros necesarios para la configuración de nuestro dominio seguro:
    - Una clave privada asociada al CSR (Al que hemos llamado server.key. El CSR no es necesario, solamente la clave privada).
    - El certificado de nuestro dominio (lo podemos llamar server.crt)
    - El certificado de la Autoridad Certificadora (lo llamaremos ca.crt).
- Es recomendable guardar estos ficheros en un lugar seguro. Por ejemplo, los almacenamos en /etc/httpd/certs/.
- Por último hay que configurar Apache para que haga uso de estos certificados. Esta sería la configuración básica:

```
<VirtualHost *:443>

    ........................

       SSLEngine on

       SSLCertificateFile /etc/httpd/certs/server.crt

       SSLCertificateKeyFile /etc/httpd/certs/server.key

       SSLCertificateChainFile /etc/httpd/certs/ca.crt

    ........................

</VirtualHost>
```

- Ya solo queda reiniciar el servicio de Apache y probar la configuración accediendo al dominio utilizando el protocolo HTTPS (https://midominio.com).

Recetas de integración

- Conexión con directorios LDAP
- Conexión con bases de datos relacionales
- Conexión con CAS
- Conexión con ADFS
- Liberación de atributos recomendados por la federación
- Personalización de la interfaz y pantalla de inicio