

SimpleSAMLphp - Configuración de conexión de Proveedor de Servicio (SP) contra Proveedor de Identidad (IdP)

Prerrequisitos

- Tener instalado simpleSAML. Las instrucciones de como hacerlo se pueden encontrar en:

<https://docs.google.com/document/d/1sunCjRxcoHMkxoEsrXRKELwXqWA360cCmvRzC77uhXU>

- Tener configurado un Proveedor de Identidad (Idp)

<https://docs.google.com/document/d/1uDUNdIEQH4m3e6429MvevktU3DLx-NzXH0CWzPz39YU>

- Tener instalado y configurado un Proveedor de Servicio (SP)

https://docs.google.com/document/d/1h4OF9lddVMpElsqmhc258n_uLN1Vv5OLrwQwd4Mnz7Y

Configuración

1. Registrar metadatos del Proveedor de Identidad (Idp) en el Proveedor de Servicio (SP)

1.1 Obtener los metadatos del Proveedor de Identidad (Idp) remoto

Utilizando el navegador de Internet ingrese a la ventana de configuración del Proveedor de Identidad (Idp) contra el que se va a conectar:

Ejemplo: 'http://ldp_remoto/simplesaml/

Seleccione la pestaña Federación. Bajo el encabezado *Metadatos IdP SAML 2.0* abra el enlace *Ver metadatos*.

Página de instalación de simpleSAMLphp

English | Bokmål | Nynorsk | Sámeigiella | Dansk | Deutsch | Svenska | Suomi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עברית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

Bienvenido

Configuración

Autenticación

Federación

Metadatos SP SAML 2.0

Entity ID: http://1 /simplesaml/module.php/saml/sp/metadata.php/default-sp
default-sp
[Ver metadatos]

Metadatos IdP SAML 2.0

Entity ID: http://Idp_remoto/simplesaml/saml2/idp/metadata.php
Index: DYNAMIC:1
[Ver metadatos]

Metadatos IdP Shib 1.3

Entity ID: http:// /simplesaml/shib13/idp/metadata.php
Index: __DYNAMIC:1__
[Ver metadatos]

Herramientas

- Borrar mis opciones de IdP en los servicios de descubrimiento de IdP
- Convertor de XML a metadatos de simpleSAMLphp

Entrar como administrador

Copyright © 2007-2014 Feide RnD

Copie el texto que está en el recuadro bajo la etiqueta “En un fichero de formato simpleSAMLphp - utilice esta opción si está usando una entidad simpleSAMLphp en el otro extremo”

```
</md: ContactPerson>  
</md: EntityDescriptor>
```

En un fichero de formato simpleSAMLphp - utilice esta opción si está usando una entidad simpleSAMLphp en el otro extremo:

Inicio metadata

```
$metadata['http://idp_remoto/simplesaml/saml2/idp/metadata.php'] = array (  
    'metadata-set' => 'saml20-idp-remote',  
    'entityid' => 'http://idp_remoto/simplesaml/saml2/idp/metadata.php',  
    'SingleSignOnService' =>  
        array (  
            0 =>  
                array (  
                    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',  
                    'Location' => 'http://idp_remoto/simplesaml/saml2/idp/SSOService.php',  
                ),  
            ),  
        ),  
    'SingleLogoutService' =>  
        array (  
            0 =>  
                array (  
                    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',  
                    'Location' => 'http://idp_remoto/simplesaml/saml2/idp/SingleLogoutService.php',  
                ),  
            ),  
        ),  
    'certData' => 'EBAgIJAPunPZyA+H1UMA0GCSqGSIb3DQEBChUAMIGOMQswCQYDVQGE  
    'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',  
);
```

Fin metadata

1.2 Registrar los metadatos copiados en el Proveedor de Servicio(SP)

- Editar el archivo de instalación del Proveedor de Servicio (SP)

```
nano /var/simplesamlphp/metadata/saml20-idp-remote.php
```

- Pegar los metadatos copiados del Idp remoto

```
<?php
```

```
$metadata['http://idp_remoto/simplesaml/saml2/idp/metadata.php'] = array (  
    'metadata-set' => 'saml20-idp-remote',  
    'entityid' => 'http://idp_remoto/simplesaml/saml2/idp/metadata.php',....  
    ...continúa...  
    'tko2SVeMgJ51J01KK8VUy+LBI+0SlrBpw/Jd6Oa2t7hPLS09729bYFSp5FHJpLK  
    DGq1yIWGYPgq4Bs7r+Mos4WgQ5L',  
    'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',  
);
```

2. Registrar en el Proveedor de Identidad remoto (IdP) el Proveedor de Servicio (SP).

El Proveedor de Identidad (Idp) necesita saber cuáles proveedores de servicios se van a conectar con el. Para esto se deben copiar los metadatos del Proveedor de Servicio (SP) y pegar en el archivo metadata/saml20-sp-remote.php. del Proveedor de Identidad.

2.1 Obtener los metadatos del Proveedor de Servicio (SP)

Utilizando el navegador de Internet ingrese a la ventana de configuración del Proveedor de Servicio (SP).

Ejemplo: 'http://**MiSP**/simplesaml/

Seleccione la pestaña Federación. Bajo el encabezado *Metadatos SP SAML 2.0* abra el enlace *Ver metadatos*.

Página de instalación de simpleSAMLphp

English | Bokmål | Nynorsk | Sámeigiella | Dansk | Deutsch | Svenska | Suomeksi | **Español** | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עברית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

Bienvenido

Configuración

Autenticación

Federación

Metadatos SP SAML 2.0

Entity ID: http://SP_Remoto/simplesaml/module.php/saml/sp/metadata.php/LocalSP

MiSP

[Ver metadatos]

Metadatos SP SAML 2.0

Entity ID: http://SP_Remoto/simplesaml/module.php/saml/sp/metadata.php/spUD

spUD

[Ver metadatos]

Metadatos IdP SAML 2.0

Entity ID: http://SP_Remoto/simplesaml/saml2/idp/metadata.php

Index: __DYNAMIC:1__

[Ver metadatos]

Metadatos IdP Shib 1.3

Entity ID: http://SP_Remoto/simplesaml/shib13/idp/metadata.php

Index: __DYNAMIC:1__

[Ver metadatos]

Herramientas

- Borrar mis opciones de IdP en los servicios de descubrimiento de IdP
- Conversor de XML a metadatos de simpleSAMLphp

Entrar como administrador



Copie el texto que esta en el recuadro bajo la etiqueta “En un fichero de formato simpleSAMLphp - utilice esta opción si está usando una entidad simpleSAMLphp en el otro extremo”

```
</md: ContactPerson>  
</md: EntityDescriptor>
```

En un fichero de formato simpleSAMLphp - utilice esta opción si está usando una entidad simpleSAMLphp en el otro extremo:

Inicio metadata

```
$metadata['http://SP_remoto/simplesaml/saml2/idp/metadata.php'] = array (  
    'metadata-set' => 'saml20-idp-remote',  
    'entityid' => 'http://SP_remoto/simplesaml/saml2/idp/metadata.php',  
    'SingleSignOnService' =>  
        array (  
            0 =>  
                array (  
                    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',  
                    'Location' => 'http://SP_remoto/simplesaml/saml2/idp/SSOService.php',  
                ),  
            ),  
        ),  
    'SingleLogoutService' =>  
        array (  
            0 =>  
                array (  
                    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',  
                    'Location' => 'http://SP_remoto/simplesaml/saml2/idp/SingleLogoutService.php',  
                ),  
            ),  
        ),  
    'certData' => '[BAGIJA PunPZYA+M1UMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYDVQQGEJ0m9nb3TDg8KhIEQuQy4xFzAVBgNVBACMDk3vZ290w4PC',  
    'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',  
);
```

Fin metadata

2.1 Registrar los metadatos en el Proveedor de Identidad (Idp)

- En el Proveedor de Identidad (IdP)

```
nano /var/simplesamlphp/metadata/saml20-sp-remote.php
```

- Pegar los metadatos obtenidos del Proveedor de servicio

```
<?php
```

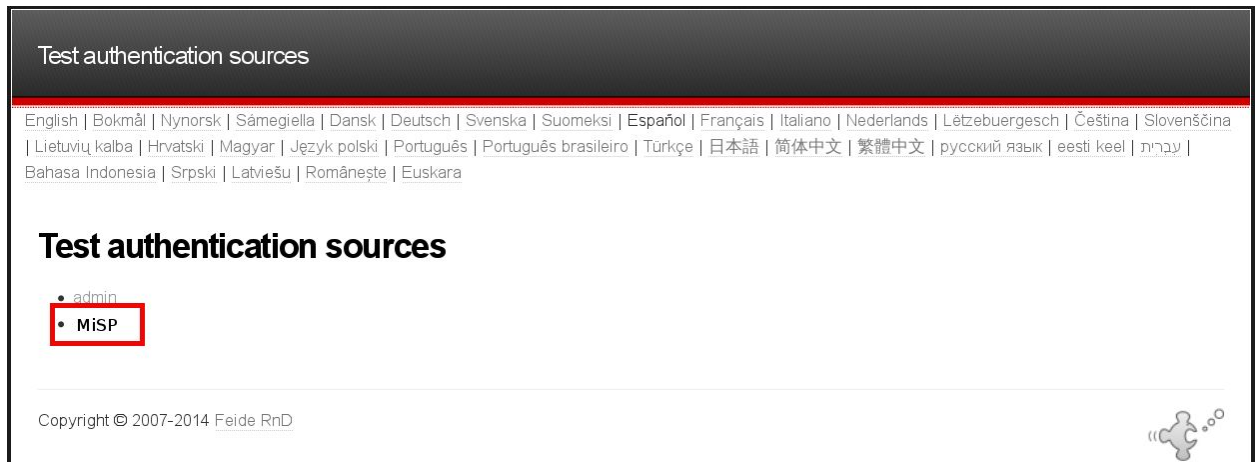
```
$metadata['http://sp_remoto/simplesaml/module.php/saml/sp/metadata.php/MiSP']  
= array (  
    'SingleLogoutService' =>  
        ...continúa...  
    'k42PRnYqfQLogM8RGoWRSPz8SA5NiEw3OdnD1pikzMwmOoUu6rg5khWdgBP',  
    ,  
);
```

Pruebas de funcionamiento

Seleccionar la pestaña autenticación en el Proveedor de Servicio



Seleccionar de la lista la fuente de autenticación el Proveedor de Servicio (SP) creado.



El sistema redirecciona a la página de autenticación del Proveedor de Identidad (Idp),
Ingresar nombre de usuario y contraseña

Indique su nombre de usuario y clave de acceso

English | Bokmål | Nynorsk | Sámeigiella | Dansk | Deutsch | Svenska | Suomeksi | **Español** | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עברית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

Indique su nombre de usuario y clave de acceso

Un servicio solicita que se autentique. Esto significa que debe indicar su nombre de usuario y su clave de acceso en el siguiente formulario.

 Nombre de usuario


 Clave de acceso

Login

¡Socorro! Se me ha olvidado mi clave de acceso.

¡Muy mal! - Sin su nombre de usuario y su clave de acceso usted no se puede identificar y acceder al servicio. A lo mejor hay alguien que puede ayudarle.
¡Póngase en contacto con el centro de ayuda de su universidad!

Copyright © 2007-2014 Feide RnD



Si el usuario y la contraseñas son correctas el Proveedor de Servicio retorna los parámetros de usuario.

Ejemplo de SAML 2.0 SP

English | Bokmål | Nynorsk | Sámeigiella | Dansk | Deutsch | Svenska | Suomeksi | **Español** | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עברית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

Ejemplo de SAML 2.0 SP

Hola, esta es la página de estado de simpleSAMLphp. Desde aquí puede ver si su sesión ha caducado, cuanto queda hasta que lo haga y todos los atributos existentes en su sesión.

Atributos

cla_codigo	20152028024
cla_clave	aee00f0c2b384f25218f8844a470a7af8463c5a2


Salir

[Salir]

Sobre simpleSAMLphp

¡Eh! Esto del simpleSAMLphp está interesante, ¿dónde puedo averiguar más? Hay más información sobre simpleSAMLphp en el blog de I+D de Feide en [UNINETT](#).

Copyright © 2007-2014 Feide RnD



Para cerrar la sesión seleccionar el enlace [[Salir](#)].



Universidad Distrital Francisco José de Caldas
Oficina Asesora de Sistemas

*Este documento está bajo licencia de Creative Commons
Reconocimiento 4.0 Internacional.*



Los nombres de programas, marcas, logotipos y citas de referencia son propiedad de sus respectivos autores y se consideran elementos conexos al documento sobre los cuales no aplican la licencia aquí declarada. Corresponde a los usuarios determinar claramente los derechos de autor que cobijan a cada uno de estos recursos.

Las ideas y expresiones contenidas en el documento corresponden a sus autores y no representan necesariamente la posición de la institución respecto a los temas tratados.