

# SimpleSAMLphp

haciendo las cosas sencillas

Victoriano Giralt

Servicio Central de Informática  
Universidad de Málaga

Antequera, 30 de junio de 2008



## 1 ¿Qué es?



# Índice

- 1 ¿Qué es?
- 2 ¿Para qué sirve?
  - Casos de uso
  - Protocolos



- 1 ¿Qué es?
- 2 ¿Para qué sirve?
  - Casos de uso
  - Protocolos
- 3 ¿Cómo está hecho?
  - Abstracción
  - Autenticación
  - Sesiones
  - Framework



- 1 ¿Qué es?
- 2 ¿Para qué sirve?
  - Casos de uso
  - Protocolos
- 3 ¿Cómo está hecho?
  - Abstracción
  - Autenticación
  - Sesiones
  - Framework
- 4 ¿Cómo funciona?
  - Escalabilidad
  - Protocolos
  - Metadatos



- 1 ¿Qué es?
- 2 ¿Para qué sirve?
  - Casos de uso
  - Protocolos
- 3 ¿Cómo está hecho?
  - Abstracción
  - Autenticación
  - Sesiones
  - Framework
- 4 ¿Cómo funciona?
  - Escalabilidad
  - Protocolos
  - Metadatos
- 5 ¿Quién?
  - Desarrolladores
  - Usuarios



# SimpleSAMLphp

a modo de definición



¿Qué es SimpleSAMLphp?



¿Qué es SimpleSAMLphp?

Es una aplicación **sencilla**



¿Qué es SimpleSAMLphp?

Es una aplicación **sencilla**  
que implementa **SAML**



¿Qué es SimpleSAMLphp?

Es una aplicación **sencilla**  
que implementa **SAML**  
en **PHP**





SimpleSAMLphp es fácil de



SimpleSAMLphp es fácil de

- instalar



SimpleSAMLphp es fácil de

- instalar:  
basta con echar un carpeta en un Apache 2 con PHP 5.2



SimpleSAMLphp es fácil de

- instalar:  
basta con echar un carpeta en un Apache 2 con PHP 5.2
- integrar



SimpleSAMLphp es fácil de

- instalar:  
basta con echar un carpeta en un Apache 2 con PHP 5.2
- integrar
- mantener



SimpleSAMLphp es fácil de

- instalar:  
basta con echar un carpeta en un Apache 2 con PHP 5.2
- integrar
- mantener
- desarrollar



# Casos de uso

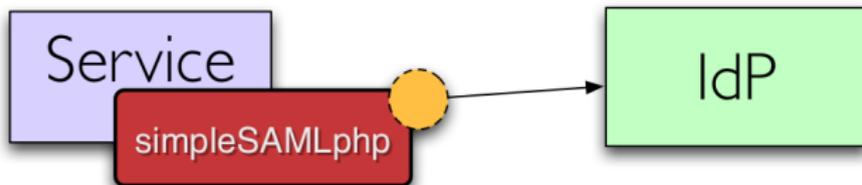
## Federar una aplicación



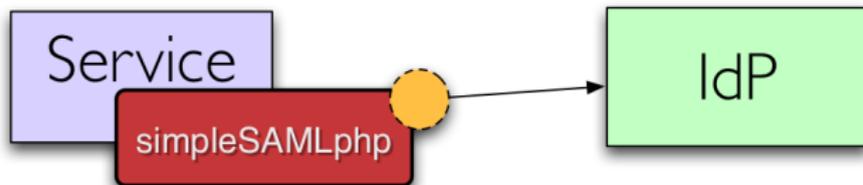
## SimpleSAMLphp para integrar aplicaciones en una federación



SimpleSAMLphp para integrar aplicaciones en una federación



SimpleSAMLphp para integrar aplicaciones en una federación



Por ejemplo: conectar un wiki a la federación



# Casos de uso

## Montar un proveedor de identidad



# Casos de uso

## Montar un proveedor de identidad

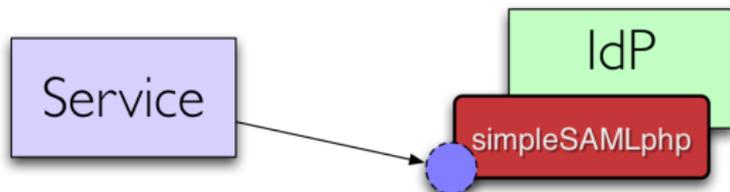
SimpleSAMLphp como proveedor de identidad de la federación



# Casos de uso

## Montar un proveedor de identidad

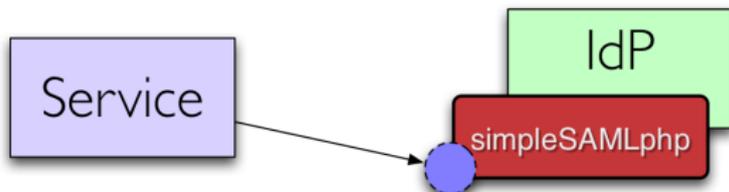
SimpleSAMLphp como proveedor de identidad de la federación



# Casos de uso

## Montar un proveedor de identidad

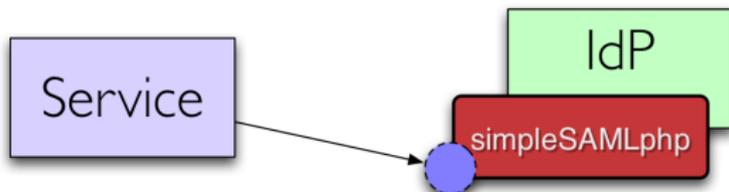
SimpleSAMLphp como proveedor de identidad de la federación



Por ejemplo:



### SimpleSAMLphp como proveedor de identidad de la federación

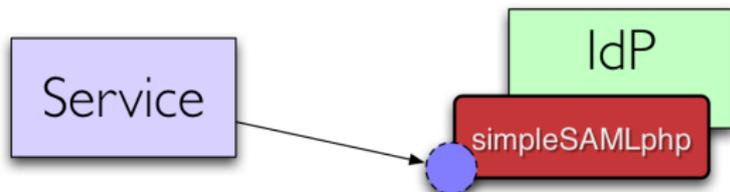


Por ejemplo:

- + El IdP de la Universidad de Málaga



### SimpleSAMLphp como proveedor de identidad de la federación

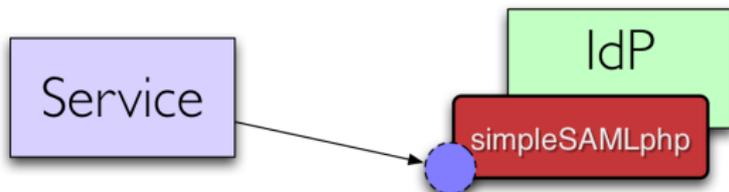


Por ejemplo:

- + El IdP de la Universidad de Málaga
- + La federación danesa wayf.dk



### SimpleSAMLphp como proveedor de identidad de la federación



Por ejemplo:

- + El IdP de la Universidad de Málaga
- + La federación danesa wayf.dk
- + Una Universidad americana que conecta a Google Apps



# Casos de uso

## Conectar protocolos



## SimpleSAMLphp para unir protocolos dispares



SimpleSAMLphp para unir protocolos dispares



SimpleSAMLphp para unir protocolos dispares



Por ejemplo:



SimpleSAMLphp para unir protocolos dispares



Por ejemplo:

Shibboleth ↔ SAML 2.0



SimpleSAMLphp para unir protocolos dispares



Por ejemplo:

Shibboleth	↔	SAML 2.0
OpenID	→	SAML 2.0



## SimpleSAMLphp para unir protocolos dispares



Por ejemplo:

Shibboleth	↔	SAML 2.0
OpenID	→	SAML 2.0
PAPI	↔	SAML 2.0



# Muchos protocolos

simpleSAMLphp es multiprotocolo



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3



SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)



SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)
- A-Select



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)
- A-Select

Próximamente:



SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)
- A-Select

Próximamente:

- WS-federation



SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)
- A-Select

Próximamente:

- WS-federation
- OAuth



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)
- A-Select

Próximamente:

- WS-federation
- OAuth
- CAS



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)
- A-Select

Próximamente:

- WS-federation
- OAuth
- CAS
- ¿Kerberos?



# Muchos protocolos

simpleSAMLphp es multiprotocolo

SimpleSAMLphp versión puede comunicarse con

Ahora (versión 1.1):

- SP SAML 2.0
- IdP SAML 2.0
- SP Shibboleth 1.3
- IdP Shibboleth 1.3
- PAPI
- OpenID (proveedor)
- A-Select

Próximamente:

- WS-federation
- OAuth
- CAS
- ¿Kerberos?
- ...



# Capas de abstracción

Abstraerse es bueno, pero con moderación



# Capas de abstracción

Abstraerse es bueno, pero con moderación

Las capas de abstracción tienen sus **ventajas**



# Capas de abstracción

Abstraerse es bueno, pero con moderación

Las capas de abstracción tienen sus **ventajas**

+ permiten extender partes del sistema fácilmente



# Capas de abstracción

Abstraerse es bueno, pero con moderación

Las capas de abstracción tienen sus **ventajas**

+ permiten extender partes del sistema fácilmente

pero también sus **inconvenientes**



# Capas de abstracción

Abstraerse es bueno, pero con moderación

Las capas de abstracción tienen sus **ventajas**

- + permiten extender partes del sistema fácilmente

pero también sus **inconvenientes**

- hacen el código más complejo, por tanto, más difícil de leer y trazar



# Capas de abstracción

Abstraerse es bueno, pero con moderación

Las capas de abstracción tienen sus **ventajas**

- + permiten extender partes del sistema fácilmente

pero también sus **inconvenientes**

- hacen el código más complejo, por tanto, más difícil de leer y trazar

Por ello, SimpleSAMLphp tiene unas pocas capas cuidadosamente escogidas



# Mecanismos de autenticación

cada uno sabe donde está su gente



# Mecanismos de autenticación

cada uno sabe donde está su gente

SimpleSAML dispone de un mecanismo de extensiones que permiten autenticar con



# Mecanismos de autenticación

cada uno sabe donde está su gente

SimpleSAML dispone de un mecanismo de extensiones que permiten autenticar con

- LDAP, de varias formas



# Mecanismos de autenticación

cada uno sabe donde está su gente

SimpleSAML dispone de un mecanismo de extensiones que permiten autenticar con

- LDAP, de varias formas
- CAS



# Mecanismos de autenticación

cada uno sabe donde está su gente

SimpleSAML dispone de un mecanismo de extensiones que permiten autenticar con

- LDAP, de varias formas
- CAS
- PostgreSQL



# Mecanismos de autenticación

cada uno sabe donde está su gente

SimpleSAML dispone de un mecanismo de extensiones que permiten autenticar con

- LDAP, de varias formas
- CAS
- PostgreSQL
- RADIUS



# Mecanismos de autenticación

cada uno sabe donde está su gente

SimpleSAML dispone de un mecanismo de extensiones que permiten autenticar con

- LDAP, de varias formas
- CAS
- PostgreSQL
- RADIUS
- PKI



# Mecanismos de autenticación

cada uno sabe donde está su gente

SimpleSAML dispone de un mecanismo de extensiones que permiten autenticar con

- LDAP, de varias formas
- CAS
- PostgreSQL
- RADIUS
- PKI
- métodos de auto registro



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP

El almacén de sesiones también es extensible:



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP

El almacén de sesiones también es extensible:

- Sesiones PHP



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP

El almacén de sesiones también es extensible:

- Sesiones PHP
- memcache



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP

El almacén de sesiones también es extensible:

- Sesiones PHP
- memcache

y permite:



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP

El almacén de sesiones también es extensible:

- Sesiones PHP
- memcache

y permite:

- Single Sign On



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP

El almacén de sesiones también es extensible:

- Sesiones PHP
- memcache

y permite:

- Single Sign On
- Single Log Out



# Manejo de sesiones

SimpleSAMLphp hereda el concepto de sesión de PHP

El almacén de sesiones también es extensible:

- Sesiones PHP
- memcache

y permite:

- Single Sign On
- Single Log Out
- almacenar atributos



# ¿Usamos un framework?

o preferimos tener más desarrolladores



# ¿Usamos un framework?

o preferimos tener más desarrolladores

¿Por qué SimpleSAMLphp no usa un framework?



# ¿Usamos un framework?

o preferimos tener más desarrolladores

¿Por qué SimpleSAMLphp no usa un framework?

- + Hay muchos frameworks buenos para PHP



# ¿Usamos un framework?

o preferimos tener más desarrolladores

¿Por qué SimpleSAMLphp no usa un framework?

- + Hay muchos frameworks buenos para PHP
- Ninguno de ellos es el mejor



# ¿Usamos un framework?

o preferimos tener más desarrolladores

¿Por qué SimpleSAMLphp no usa un framework?

- + Hay muchos frameworks buenos para PHP
- Ninguno de ellos es el mejor
- Cuesta más entrar en el desarrollo



# ¿Usamos un framework?

o preferimos tener más desarrolladores

¿Por qué SimpleSAMLphp no usa un framework?

- + Hay muchos frameworks buenos para PHP
- Ninguno de ellos es el mejor
- Cuesta más entrar en el desarrollo
- Tienen más requisitos para instalar



# ¿Usamos un framework?

o preferimos tener más desarrolladores

¿Por qué SimpleSAMLphp no usa un framework?

- + Hay muchos frameworks buenos para PHP
- Ninguno de ellos es el mejor
- Cuesta más entrar en el desarrollo
- Tienen más requisitos para instalar

SimpleSAMLphp no usa frameworks para que sea fácil tanto de desarrollar como de desplegar



# ¿Puede crecer?

SimpleSAML puede cubrir casi cualquier necesidad



# ¿Puede crecer?

SimpleSAML puede cubrir casi cualquier necesidad

Es más fácil escalar usando medios simples que complicados



# ¿Puede crecer?

SimpleSAML puede cubrir casi cualquier necesidad

Es más fácil escalar usando medios simples que complicados

desde algo sencillo



# ¿Puede crecer?

SimpleSAML puede cubrir casi cualquier necesidad

Es más fácil escalar usando medios simples que complicados

desde algo sencillo

Apache 2 + PHP 5

simpleSAMLphp



# ¿Puede crecer?

SimpleSAML puede cubrir casi cualquier necesidad

Es más fácil escalar usando medios simples que complicados

a algo no tan sencillo

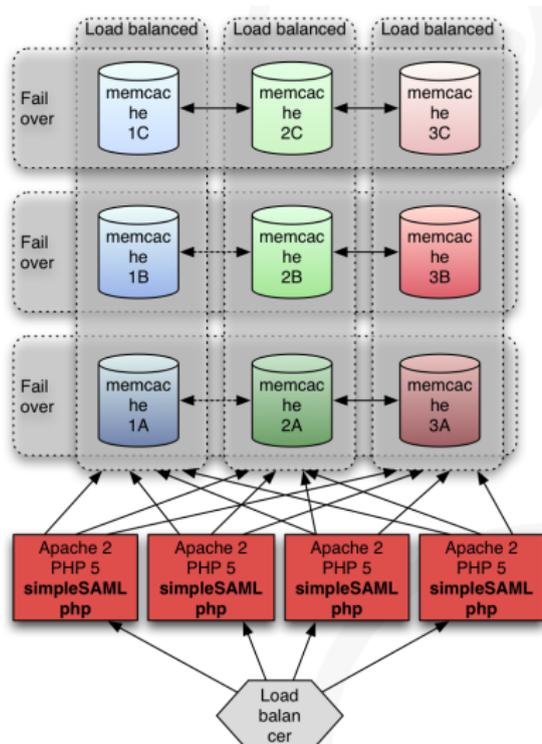


# ¿Puede crecer?

SimpleSAML puede cubrir casi cualquier necesidad

Es más fácil escalar usando medios simples que complicados

a algo no tan sencillo



# Protocolos XML

simplificando la complejidad



SimpleSAMLphp maneja el XML con su simplicidad habitual



SimpleSAMLphp maneja el XML con su simplicidad habitual

- Plantillas de texto para enviar



SimpleSAMLphp maneja el XML con su simplicidad habitual

- Plantillas de texto para enviar  
fácil de rellenar con parámetros y atributos



SimpleSAMLphp maneja el XML con su simplicidad habitual

- Plantillas de texto para enviar  
fácil de rellenar con parámetros y atributos
- XPath para recibir



SimpleSAMLphp maneja el XML con su simplicidad habitual

- Plantillas de texto para enviar  
fácil de rellenar con parámetros y atributos
- XPath para recibir  
flexible y eficaz, coge lo que necesita e ignora el resto



# Gestión de metadatos

SimpleSAMLphp facilita la gestión de los metadatos



# Gestión de metadatos

SimpleSAMLphp facilita la gestión de los metadatos

La gestión de metadatos de SimpleSAMLphp es muy moderna



# Gestión de metadatos

SimpleSAMLphp facilita la gestión de los metadatos

La gestión de metadatos de SimpleSAMLphp es muy moderna

- IdPs y SPs generan sus metadatos *al vuelo*



# Gestión de metadatos

SimpleSAMLphp facilita la gestión de los metadatos

La gestión de metadatos de SimpleSAMLphp es muy moderna

- IdPs y SPs generan sus metadatos *al vuelo*
- La instalación incluye metadatos de algunas federaciones



# Gestión de metadatos

SimpleSAMLphp facilita la gestión de los metadatos

La gestión de metadatos de SimpleSAMLphp es muy moderna

- IdPs y SPs generan sus metadatos *al vuelo*
- La instalación incluye metadatos de algunas federaciones
- Se está trabajando en metadatos dinámicos



# Comunidad

los usuarios son desarrolladores



SimpleSAMLphp es un proyecto OpenSource, por tanto



SimpleSAMLphp es un proyecto OpenSource, por tanto

- Todo el mundo puede participar



SimpleSAMLphp es un proyecto OpenSource, por tanto

- Todo el mundo puede participar
- Los usuarios ayudan a otros usuarios



SimpleSAMLphp es un proyecto OpenSource, por tanto

- Todo el mundo puede participar
- Los usuarios ayudan a otros usuarios
- Los usuarios pueden influir en el desarrollo



SimpleSAMLphp es un proyecto OpenSource, por tanto

- Todo el mundo puede participar
- Los usuarios ayudan a otros usuarios
- Los usuarios pueden influir en el desarrollo
- Muchos hemos contribuido en mayor o menor medida



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)
- CONFIA(.es)



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)
- CONFIA(.es) ¿verdad?



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)
- CONFIA(.es) ¿verdad?
- Unos pocos de americanos



# ¿Quién lo está usando?

SimpleSAMLphp se extiende como el fuego en la sabana

Los usuarios de SimpleSAMLphp aumentan a diario

- FEIDE(.no)
- WAYF.dk
- SWAMI(.se)
- Kalmar(.dk+.fi+.no+.se)
- DFN-AAI(.de)
- CONFIA(.es) ¿verdad?
- Unos pocos de americanos
- ...



## SimpleSAMLphp

- es fácil de desplegar y usar



## SimpleSAMLphp

- es fácil de desplegar y usar
- permite montar federaciones muy rápido



## SimpleSAMLphp

- es fácil de desplegar y usar
- permite montar federaciones muy rápido
- es multiprotocolo



## SimpleSAMLphp

- es fácil de desplegar y usar
- permite montar federaciones muy rápido
- es multiprotocolo
- es multilingüe



## SimpleSAMLphp

- es fácil de desplegar y usar
- permite montar federaciones muy rápido
- es multiprotocolo
- es multilingüe
- <http://rnd.feide.no/simplesamlphp>

