# simpleSAMLphp

Implementazione SP a livello applicativo

Marco Ferrante – Università di Genova/CTS IDEM

# SimpleSAMLphp (ssp)

È una libreria/framework php sviluppato dalla rete norvegese per la ricerca https://www.uninett.no/en

Rispetto alle soluzioni basate su Shibboleth SP:

- non richiede interventi a livello di sistema
- può essere portato con l'applicazione

# Riferimenti

https://simplesamlphp.org/docs/1.12/saml:sp

https://www.idem.garr.it/documenti/doc_view/312-installazione-simplesamlphp-service-provider-su-debian-linux

# Installazione

Istruzioni relative alla versione 1.12/1.13

PHP version >= 5.3.0

https://simplesamlphp.org/

cd /var

tar xzf simplesamlphp-1.x.y.tar.gz

mv simplesamlphp-1.x.y simplesamlphp

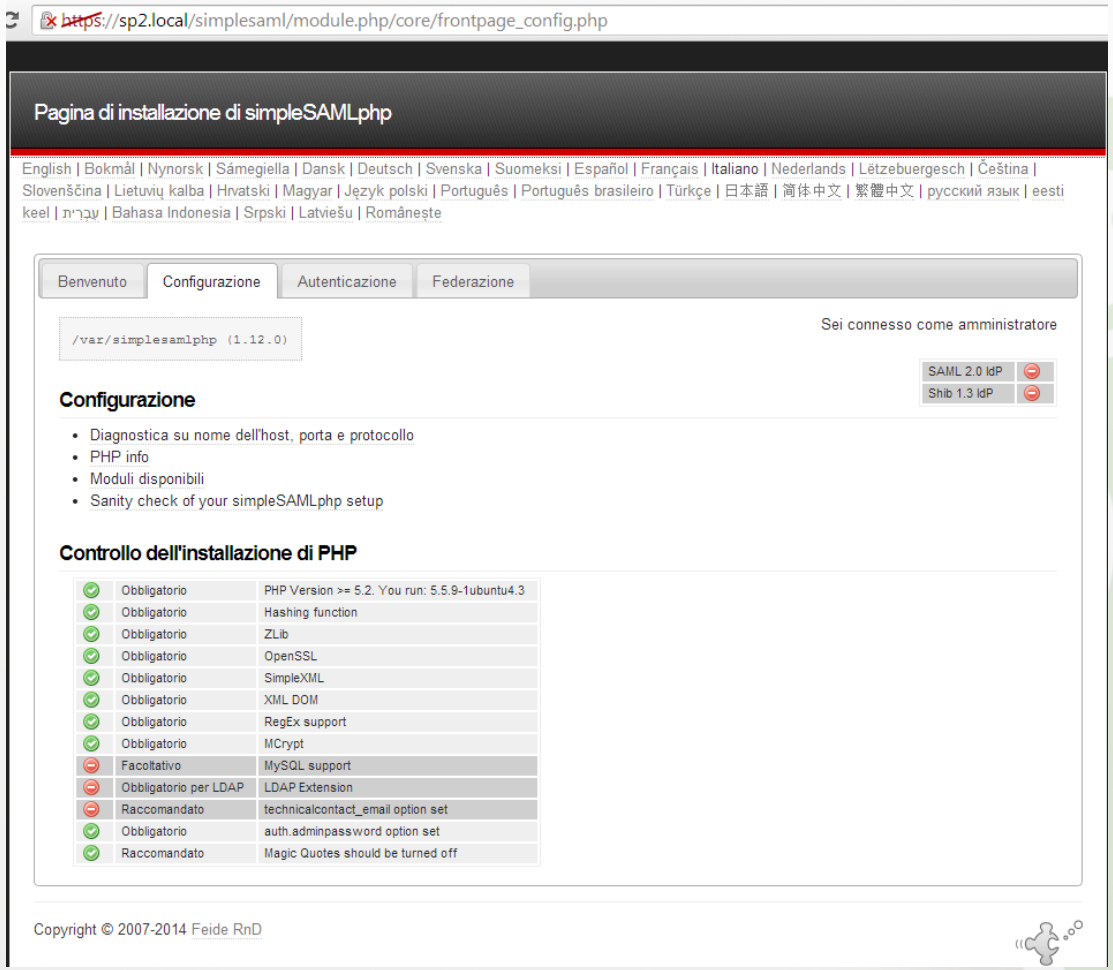
(le librerie stanno migrando a Composer)

# Apache

```
<VirtualHost *>
...
        Alias /simplesaml /var/simplesamlphp/www
  # Apache 2.4
   <Directory /var/simplesamlphp/www>
        Require all granted
    </Directory>
</VirtualHost>
```

# Autodiagnosi

Aprire:
https://sp1.local/simplesaml/



# Configurazione generale

File di configurazione e metadati sono in PHP

Editare */var/simplesamlphp/config/config.php*

```
'auth.adminpassword' => ...
'secretsalt' => ….
'technicalcontact_name' => 'Supporto Tecnico',
'technicalcontact_email' => 'idem-corso@garr.it',
'language.default' => 'it',
'timezone' => 'Europe/Rome',
```

# Registrare l'IdP

I metadati dell'IdP/federazione vanno salvati in *metadata/saml20-idp-remote.php*

Possibile editarli a mano:

```
$metadata['https://idp-corso.irccs.garr.it/idp/shibboleth'] =
array(
    'name' => array(
          'it' => 'IdP di test per il corso',
    ),
    'SingleSignOnService' =>
'https://idp-corso.irccs.garr.it/idp/profile/SAML2/Redirect/SSO',
    'certFingerprint' => 'BF:3E:8D:4C:7A:ED:C2:D1:61:20:00:9B:
19:B7:C9:FA:44:27:9D:61',
);
```

# Registrare i metadati IDEM

Per la federazione, ssp fornisce un tool di conversione XML → PHP

Comprende un modulo (metarefresh) per l'aggiornamento automatico

# Certificato SP

Chiave e certificato vanno in *cert/*

```
cp /etc/shibboleth/sp-key.pem /var/simplesamlphp/cert/
cp /etc/shibboleth/sp-cert.pem /var/simplesamlphp/cert/
chown www-data /var/simplesamlphp/cert/sp-key.pem
```

# Configurazione SP

Editare *config/authsources.php*

```
'sp-idem' => array(
    'saml:SP',
    'entityID' => 'https://sp2.local/
simplesaml',
    'privatekey' => 'sp-key.pem',
    'certificate' => 'sp-cert.pem',
    'idp' => NULL,  // Specificare un IdP
    'discoURL' => NULL,
       // Specificare un Discovery Service
    ...
```

# Discovery Service

```
'idp' => 'entityID IdP',
```

Redirige direttamente all'IdP (Web SSO senza DS)

```
'discoURL' => 'https://wayf.idem-test...',
```

Redirige al servizio di CDS

```
'idp' => NULL, 'discoURL' => NULL
```

Usa un EDS “basic”

# EDS

Presenta l'elenco degli IdP in *metadata/saml20-idp-remote.php*

# Metadati SP

```
...
'OrganizationName' => 'IDEM',
'OrganizationDisplayName' =>
    'Federazione IDEM',
'OrganizationURL' =>
    'http://www.idem.it',
...
```

# Metadati UI per IDEM

```
    ...
    'UIInfo' => array(
        'DisplayName' => array(
            'en' => 'SP Single Sign-on
(ssp)',
            'it' => 'SP Single Sign-on
(ssp)'
        ),
        'Description' => array(
            'it' => 'Service Provider di
Esempio per il corso  "Abilitare le
applicazioni web al Single Sign-on con
strumenti SAML" (versione ssp)'
```

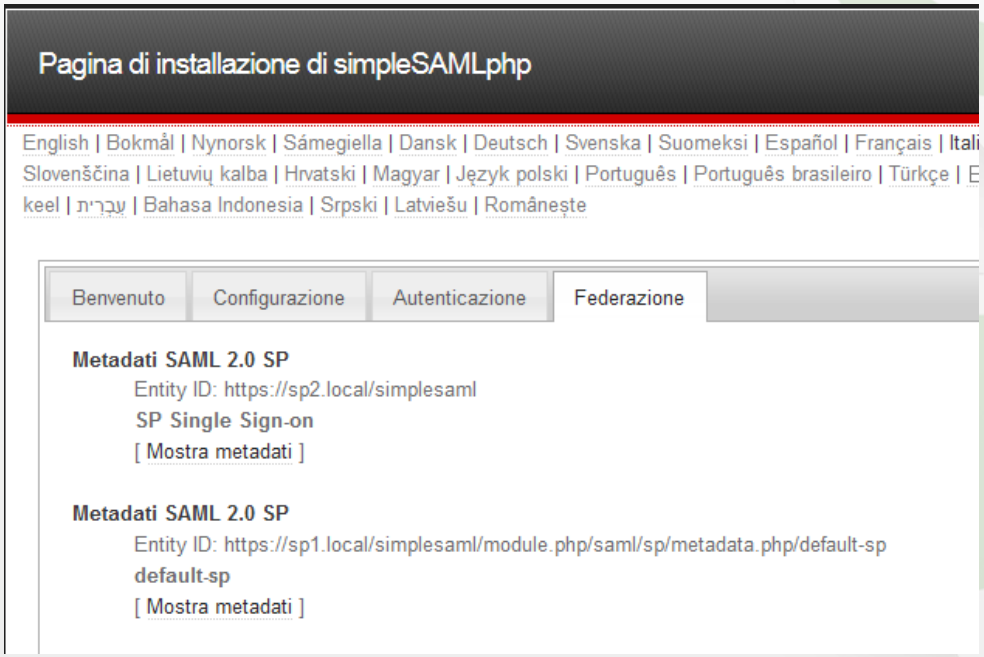
# Requested attributes

Servono entrambi per includerli nei metadati

```
...
'attributes' =>
    array('eduPersonEntitlement',
        'mail'),
'name' => array('it' =>
        'SP Single Sign-on'),
...
```

# Recupero dei metadati

- Tab “Federazione” della pagina di amministrazione
- Inviarli a IDEM o caricarli sull'IdP



# Autenticazione da PHP

```
<?php
require_once('/var/simplesamlphp/lib/
_autoload.php');
$as = new SimpleSAML_Auth_Simple('sp-idem');
if (!$as->isAuthenticated()) {
    $as->login();
}
$attributes = $as->getAttributes();
print_r($attributes);
```

# Troubleshooting

Usare la pagina di test

Attivare il logging:

editare *config/config.php*

```
'debug' => TRUE,
'logging.level' => SimpleSAML_Logger::INFO,
'logging.handler' => 'file',
```

chown www-data log/

# Attributi

Gli attributi sono restituiti come array

- Nessun problema con gli attributi multivalore

Possono essere manipolati da filtri post-auth

```
'authproc' => array(
    // Da OID a friendlyNames
    90 => array('class' =>
        'core:AttributeMap','oid2name'),
    ),
```

# Configurazione alternativa

Cambiare directory

```
<?php
require_once('/var/simplesamlphp/lib/
_autoload.php');
SimpleSAML_Configuration::setConfigDir('/
tmp');
$as = new SimpleSAML_Auth_Simple('sp-idem');
...
```

# Config override

```
$config = array (
    'override.host' => array(
        'sp.andreas.feide.no' =>
'config.test.php',
        'sp1.anderas.feide.no' =>
'config.test.php',
        'sp2.anderas.feide.no' =>
'config.test.php',
    ),
```