Fundação para a Computação Científica Nacional
*Foundation for National Scientific Computing*

# Cookbook – SimpleSAMLphp Service Provider

## Serviço Utilizador RCTS
## Fevereiro de 2010

05 de Fevereiro de 2010

UMIC
FCCN Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing
RCTS
Financiado por:

Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

# Cookbook – SimpleSAMLphp Service Provider

## Serviço Utilizador RCTS
## Fevereiro de 2010

EXT/2010/Serviço Utilizador RCTS

| Versão | Data | Autor |
|---|---|---|
| 1.0 | 01-02-2010 | Esmeralda Câmara |
| 1.1 | 04-02-2010 | IST, Miguel Cabeça |
| 1.2 | 05-02-2010 | Esmeralda Câmara |

# ÍNDICE

**1 INTRODUÇÃO ..... 1**
1.1 Objectivos ..... 1

**2 INSTALAÇÃO – SIMPLESAMLPHP SP ..... 2**
2.1 Software e Pré-requisitos ..... 2
2.2 Processo de Instalação ..... 3

**3 CERTIFICADOS SSL ..... 4**

**4 APACHE - CONFIGURAÇÃO ..... 5**

**5 SIMPLESAMLPHP SP - CONFIGURAÇÃO GERAL ..... 6**
5.1 Directório Base ..... 6
5.2 Site de Administração ..... 7
5.3 Directório de Metadados ..... 8

**6 SIMPLESAMLPHP SP - METADADOS DA FEDERAÇÃO ..... 10**
6.1 Módulo Cron ..... 10
6.2 Módulo "Metarefresh" ..... 11

**7 SIMPLESAMLPHP SP - ATRIBUTOS E METADADOS ..... 13**
7.1 SP EntityID e Atributos ..... 13
7.2 SP Metadados ..... 15

**8 PONTOS DE CONTACTO ..... 16**

**9 ANEXOS ..... 17**
9.1 Criar Certificado SSL ..... 17

**10 REFERÊNCIAS ..... 19**

# 1 INTRODUÇÃO

O SimpleSAMLphp é uma implementação simples do SAML 2.0 em PHP nativo (suportado por Linux,UNIX,Mac OSX, Windows) e permite a configuração de ambos e componentes "Identity Provider" e "Service Provider". A configuração "Service Provider SimpleSAMLphp" permite comunicar e delegar a autenticação a Identity Provider's Shibboleth ou SAML2.0 IdP.

## 1.1 OBJECTIVOS

Este documento pretende descrever uma instalação "SimpleSAMLphp Service Provider" e a respectiva configuração para integrar o componente na federação de testes.

# 2 INSTALAÇÃO – SIMPLESAMLPHP SP

## 2.1 SOFTWARE E PRÉ-REQUISITOS

Antes de dar inicio à instalação e configuração do "Service Provider" é necessário verificar se os seguintes pré-requisitos estão assegurados:

- ✓ **Apache HTTP 2.2 com mod-ssl**

  Servidor Aplicacional Web que desempenha as funções de frontend do SP. Para configuração, consulte a documentação Apache HTTP nas referências.

- ✓ **OpenSSL**

  Para concretizar funcionalidades de SSL e garantir a privacidade dos dados. Também utilizada na criação de certificados. Directamente interligado com o Apache2.

- ✓ **NTP**

  Os servidores devem estar sincronizados para evitar erros "clock-skew".

- ✓ **PHP >= 5.2.0**

  Extensões PHP necessárias: `date`, `dom`, `hash`, `libxml`, `openssl`, `pcre`, `SPL`, `zlib`

- ✓ **SimpleSAMLphp**

  A versão mais recente do simpleSAMLphp encontra-se no seguinte url: ***http://code.google.com/p/simplesamlphp/***

## 2.2 PROCESSO DE INSTALAÇÃO

```
cd /var

wget http://simplesamlphp.googlecode.com/files/simplesamlphp-1.5.1.tar.gz

tar xzf simplesamlphp-1.5.1.tar.gz

mv simplesamlphp-1.5.1 simplesamlphp
```

# 3 CERTIFICADOS SSL

Devem ser criados dois certificados SSL com o objectivo de preservar a confidencialidade dos dados utilizados na comunicação entre o SP, IDP e o *browser* do cliente. O SP Web Server deve gerir as suas próprias chaves e certificados para estabelecer ligações TLS/SSL com o browser do cliente. Apesar de tecnicamente possível que o software do SP utilize o mesmo par de chaves e certificados do Web Server, não é recomendado que sejam utilizados os mesmos por razões de segurança.

- Certificados para o SimpleSAMLphp SP: **sp.key**
- Certificados para o SP Web Server: **your_sp_hostname.pt.key**

Para a criação de certificados consulte o anexo 9.1

# 4 APACHE - CONFIGURAÇÃO

Aceder ao ficheiro httpd.conf e associar o simpleSAMLphp ao virtual host do serviço através de um "alias" para o directório de instalação do simpleSAMLphp.

```
Listen 443
#
# SERVICE PROVIDER SSL Virtual hosts
#
<VirtualHost *:443>
SSLEngine on
ServerName your_sp_hostname.pt
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
SSLOptions +StdEnvVars +ExportCertData
SSLCertificateFile /path/to/your/your_sp_hostname.pt.crt
SSLCertificateKeyFile /path/to/your/your_sp_hostname.pt.key
DocumentRoot /home/httpd/your_sp_hostname/html

DirectoryIndex index.php
Alias /simplesaml /var/simplesamlphp/www

<Directory "/home/httpd/your_sp_hostname.pt/html">
Options Indexes FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
# Logs do Site
ErrorLog /home/httpd/your_sp_hostname/logs/error_log
CustomLog /home/httpd/your_sp_hostname/logs/access_log combined
<VirtualHost>
```

Nota: Os portos 443 (https) e 80(http) devem ser abertos na *firewall* e a aceitar pedidos TCP.

# 5 SIMPLESAMLPHP SP - CONFIGURAÇÃO GERAL

Os simpleSAMLphp contem de ficheiros de configuração "template" que devem ser copiados para as respectivas directorias.

```
cd /var/simplesamlphp
cp -r config-templates/*.php config/
cp -r metadata-templates/*.php metadata/
```

O ficheiro /var/simplesamlphp/config/config.php é responsável pela configuração geral do simpleSAMLphp.

## 5.1 DIRECTÓRIO BASE

Ficheiro: /var/simplesamlphp/config/config.php

Por omissão é considerado como directório base o /var/simplesamlphp/

```
<?php
/*
 * The configuration of simpleSAMLphp
 *
 * $Id: config.php 1881 2009-10-20 09:14:47Z olavmrk $
 */

$config = array (

        /**
         * Setup the following parameters to match the directory of your
installation.
         * See the user manual for more details.
         */
        'baseurlpath'           => 'simplesaml/',
        'certdir'               => 'cert/',
        'loggingdir'            => 'log/',
        'datadir'               => 'data/',

        /*
         * A directory where simpleSAMLphp can save temporary files.
         *
         * SimpleSAMLphp will attempt to create this directory if it doesn't
exist.
         */
         'tempdir'               => '/tmp/simplesaml',
…
```

## 5.2 SITE DE ADMINISTRAÇÃO

O simpleSAMLphp disponibiliza um interface que permite avaliar a configuração do "Service Provider". Para aceder à zona privada é necessário realizar login com a palavra-chave configurada no ficheiro /var/simplesamlphp/config/config.php.

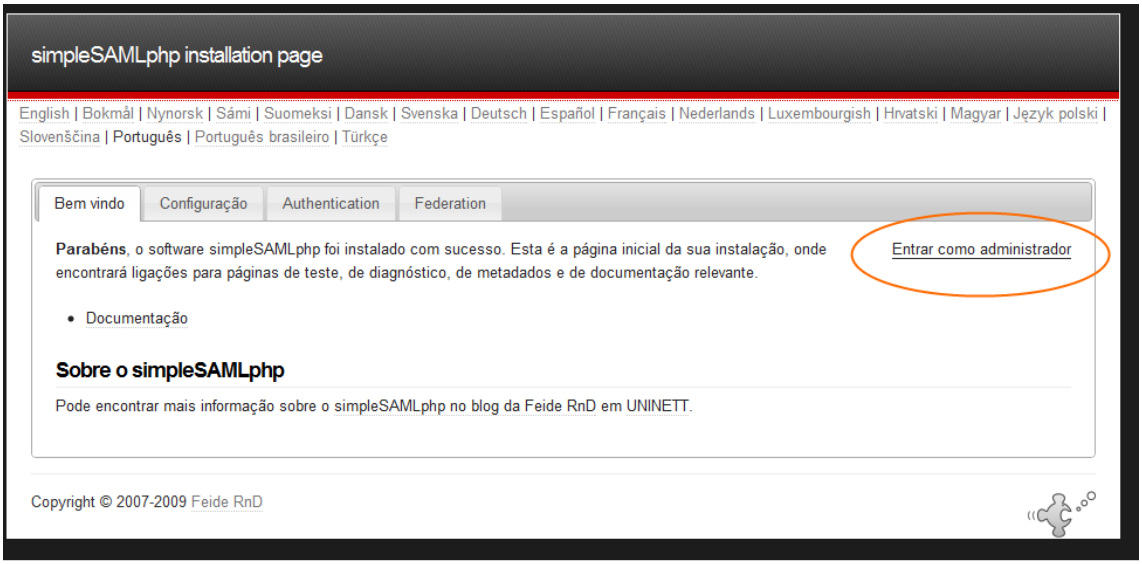
```
/**
* This password must be kept secret, and modified from the default value 123.
* This password will give access to the installation page of simpleSAMLphp with
* metadata listing and diagnostics pages.*/
        'auth.adminpassword'          => 'Palavra-Chave',
        'admin.protectindexpage'      => false,
        'admin.protectmetadata'               => false,
 /**
* This is a secret salt used by simpleSAMLphp when it needs to generate a secure hash
* of a value. It must be changed from its default value to a secret value. The value
of
* 'secretsalt' can be any valid string of any length.
*
* A possible way to generate a random salt is by running the following command from a
unix shell:
* tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1
2>/dev/null;echo
*/
        'secretsalt' => 'random_string_inserir_aqui',


/*
* Some information about the technical persons running this installation.
* The email address will be used as the recipient address for error reports, and
* also as the technical contact in generated metadata.
*/
        'technicalcontact_name'     => 'Primeiro e Ultimo Nome do Admin. do SP',

        'technicalcontact_email'    => 'sp_admin_email@instituicao.pt',
```

O valor a colocar no campo "secretsalt" é utilizado pelo SimpleSAMLphp para gerar hashes seguras e deve corresponder a uma string aleatória. O comando sublinhado a azul permite em sistemas Unix gerar a respectiva string.

Para aceder ao site de administração: **https://your_sp_hostname.pt/simplesaml**




## 5.3 DIRECTÓRIO DE METADADOS

No directório /var/simplesamlphp/metadata podemos encontrar os ficheiros que identificam os componentes remotos considerados de confiança à federação, ou seja os metadados. Porque o simpleSAMLphp permite ser utilizado em simultâneo como Service Provider e Identity Provider, é necessário configurar ficheiros distintos dependendo do componente que se está a configurar.

Quando se trata da configuração de um **"*Service Provider*"** é necessário configurar os seguintes ficheiros:

- ✓ **/var/simplesamlphp/authsources.php**
  Neste ficheiro permite identificar o EntityID do SP e respectivos atributos que devem ser mapeados para o serviço.

- ✓ **/var/simplesamlphp/saml20-idp-remote.php**
  Este ficheiro permite configurar os "Identity Provider's" remotos que pertencem à federação e que podem utilizar o serviço.

No ficheiro de configuração geral é necessário identificar o directório onde o simpleSAMLphp pode encontrar o ficheiro **saml20-idp-remote.php**.

**Ficheiro:** /var/simplesamlphp/config/config.php

```
* Default:
* 'metadata.sources' => array(
* array('type' => 'flatfile')
* ),
*/
'metadata.sources' => array(
        array('type' => 'flatfile'),
        array('type' => 'flatfile', 'directory' =>
                    'metadata/rctsaai'),
),


/*
```

Segundo esta configuração o simpleSAMLphp vai procurar o ficheiro saml20-idp-remote.php nos seguintes directórios:

- ✓ /var/simplesamlphp/metadata
- ✓ /var/simplesamlphp/metadata/rctsaai

Recomendamos a seguinte configuração:

Criar o directório **rctsaai** em /var/simplesamlphp/metadata para guardar o ficheiro saml20-idp-remote.php. O simpleSAMLphp permite gerar o ficheiro remoto (saml20-idp-remote.php) de forma automática tendo por base o ficheiro de metadados da federação através dos módulos"cron" e "metarefresh". A configuração destes módulos encontra-se na secção 6.

# 6 SIMPLESAMLPHP SP - METADADOS DA FEDERAÇÃO

O SimpleSAMLphp permite a actualização periódica de metadados (saml20-idp-remote.php) de forma automática através dos módulos cron e metarefresh.

O módulo cron percorre todos os módulos activos e executa as tarefas necessárias existentes no seguinte directório de cada módulo:

/var/simplesamlphp/modules/<nome_modulo>/hooks/hooks_cron.php

O módulo metarefresh é responsável por criar o ficheiro saml20-idp-remote.php com base no link de metadados configurado no modulo.

## 6.1 MÓDULO CRON

**Passo I - Activar Módulo CRON**

```
cd /var/simplesamlphp/modules/cron
touch enable
cp config-templates/*.php ../../config/
```

**Passo II - Configurar o módulo**

```
cd /var/simplesamlphp/config
vi module_cron.php
```

```
<?php
        $config = array (
                'key' => 'SECRET',
                'allowed_tags' => array('daily', 'hourly',
                'frequent'),
                'debug_message' => TRUE,
                'sendemail' => TRUE,
        );

?>
```

**Passo III – Adicionar comandos do módulo na "crontab"**

Aceder ao seguinte url:

**https://your_sp_hostname.pt/simplesaml/module.php/cron/croninfo.php**

Copiar da página as sugestão para a crontab (adicionar a cada comando a opção –k para ignorar o certificado).

```
crontab -e


# Run cron [daily]
02 0 * * * curl -k -silent
"https://your_sp_hostname.pt/simplesaml/module.php/cron/cron.php?key=SECRET=daily"    >
/dev/null 2>&1
# Run cron [hourly]
01 * * * * curl -k -silent
"https://your_sp_hostname.pt/simplesaml/module.php/cron/cron.php?key=SECRETtag=hourly"
> /dev/null 2>&1
# Run cron [frequent]
XXXXXXXXXX curl -k -silent
"https://your_sp_hostname.pt/simplesaml/module.php/cron/cron.php?key=SECRET&tag=frequen
t" > /dev/null 2>&1
```

## 6.2 MÓDULO "METAREFRESH"

### Passo I - Activar modulo metarefresh

```
cd /var/simplesamlphp/modules/metarefresh
touch enable
cp config-templates/*.php ../../config/
```

### Passo II – Configurar o módulo

```
cd /var/simplesamlphp/config/
vi config-metarefresh.php
```

```
<?php
        $config = array( 'sets' => array(
                'rctsaai' => array(
                        'cron' => array('hourly'),
                        'sources' => array(
                        array(
                                'src'                                          =>
                                'http://metadatarctsaai.fccn.pt/metadata/RCTSaai
                                _testbedmetadata.xml'
                                ),
                        ),
                        'maxCache' => 60*60*24*4, // Maximum 4 days cache
        time.
                        'maxDuration'  =>  60*60*24*10,  //  Maximum  10  days
                        duration on
                        ValidUntil.
```

```
                        'outputDir' => 'metadata/rctsaai/',
                ),
        ));
?>
```

**Nota:** Adicionar permissões de escrita para o Apache para escrever no directório metadata/rctsaai

# 7 SIMPLESAMLPHP SP - ATRIBUTOS E METADADOS

## 7.1 SP ENTITYID E ATRIBUTOS

O ficheiro authsources.php localizado no directório /var/simplesamlphp/config é responsável por identificar o entityId do "Service Provider" e mapear os respectivos atributos provenientes do "Identity Provider".

```
<?php
/*
 * SAML 2.0 Meta data for simpleSAMLphp
 <?php

$config = array(

        // This is a authentication source which handles admin authentication.
        'admin' => array(
                // The default is to use core:AdminPassword, but it can be replaced with
                // any authentication source.

                'core:AdminPassword',
        ),

// An authentication source which can authenticate against both SAML 2.0
// and Shibboleth 1.3 IdPs.

      'YOUR_SP_ID' => array(

                'saml:SP',

// The entity ID of this SP.
// Can be NULL/unset, in which case an entity ID is generated based on the metadata URL.
                'entityID' => 'https://your_sp_hostname.pt',

 // The entity ID of the IdP this should SP should contact.
// Can be NULL/unset, in which case the user will be shown a list of available IdPs.
                'idp' => NULL,

                // The URL to the discovery service.
                // Can be NULL/unset, in which case a builtin discovery service will be
used.
                'discoURL' =>  'https://wayf.fccn.pt/FCCNdesenvolvimento/',

                 'certificate' => 'sp.crt',
                 'privatekey'  => 'sp.key',
                 'privatekey_pass' => 'password',
                 'NameIDPolicy'                  =>'urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified',

                 'authproc' => array(
                                            50 => array(
                                        'class' => 'core:AttributeMap',
                                        'urn:oid:2.5.4.3' => 'username',
                                        'urn:oid:0.9.2342.19200300.100.1.3' => 'mail',
                                        'urn:oid:2.5.4.4' => 'surname',
                                        'urn:oid:2.5.4.42' => 'givenname',
                                        'urn:oid:2.5.4.10' => 'o'))
      ),
);
?>
```

Para adicionar um Service Provider é necessário acrescentar um elemento no array identificado por uma chave 'YOU_SP_ID'.

Este novo elemento é também um array composto por parâmetros que definem o SP tais como o entityID. É também neste array que podemos associar o serviço WAYF através do parâmetro 'discoURL' => 'https://wayf.fccn.pt/FCCNdesenvolvimento/'.

O sp.crt é o certificado utilizado quando é gerada a metadata do SP. O sp.key é utilizado para assinar e decifrar as mensagens do IdP. Por omissão o simpleSAMLphp procura estes ficheiros no directório /var/simplesamlphp/cert/.

Recomenda-se uma cópia dos ficheiros para este localização ou a criação de um symblink .( ex.: ln –s /etc/ssl/private/sp.key /var/simplesamlphp/cert/)

A configuração dos atributos é realizada através dos chamados "Auth Proc Filters" que se encontram representados no elemento "authproc" e pode ser utilizado para filtrar (core:AttributeFilter) e mapear (core:AttributeMap) atributos. Estas operações são realizadas de acordo com a prioridade associada no index do array.

```
'authproc' => array(
                    50 => array(
                'class' => 'core:AttributeMap',
                'urn:oid:2.5.4.3' => 'username',
                'urn:oid:0.9.2342.19200300.100.1.3' => 'mail',
                'urn:oid:2.5.4.4' => 'surname',
                'urn:oid:2.5.4.42' => 'givenname',
                'urn:oid:2.5.4.10' => 'o')
)
```

O exemplo acima é referente ao mapeamento de atributos proveniente do "Identity Providers" no formato "oid" para os respectivos nomes a utilizar nas variáveis de sessão da aplicação.

Para integrar os atributos do Service Provider simpleSAMLphp numa aplicação php é necessário adicionar as seguintes linhas:

```
require_once('../../lib/_autoload.php');
$as = new SimpleSAML_Auth_Simple('YOUR_SP_ID');
$as->requireAuth();
$attributes = $as->getAttributes();
print_r($attributes);
```

Para aplicações desenvolvidas em outras linguagens que não o php é recomendado a utilização de um módulo Apache v2 o Auth MemCookie. Para mais informações sobre este módulo pode consultar os seguintes links:

- ✓ http://authmemcookie.sourceforge.net/
- ✓ http://rnd.feide.no/content/simplesamlphp-advanced-features

## 7.2 SP METADADOS

Para adicionar o "Service Provider" no ficheiro de metadados da federação é necessário aceder ao seguinte link:

Realize uma cópia do conteúdo em xml e envie por email para rctsaai@fccn.pt.

# 8 PONTOS DE CONTACTO

Para questões relacionadas com o componente "Service Provider" , envie uma mensagem de correio electrónico para rctsaai@fccn.pt.

# 9 ANEXOS

## 9.1 CRIAR CERTIFICADO SSL

Deverá ser gerado um certificado SSL no seu "Service Provider" com o objectivo de preservar a confidencialidade dos dados utilizados na autenticação e autorização.

```
Atribuindo como exemplo de FQDN o url www.virtualhost.pt.

Para gerar a chave (secret ficheiro .key):

openssl genrsa -des3 -out www.virtualhost.pt.key 1024
```

```
Será criado um output do género:

Generating RSA private key, 1024 bit long modulus

................++++++

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

.....................++++++

e is 65537 (0x10001)

Enter pass phrase for www.virtualhost.pt.key:

(Onde deverá colocar uma passphrase para a geração da sua chave.)

Verifying - Enter pass phrase for www.virtualhost.pt.key:

(E repetindo a passphrase para confirmação.)

No final é criado o ficheiro .key com a sua chave privada de certificado.

 www.virtualhost.key
```

Para emitir um pedido de certificado a uma "Certificate Authority" deverá criar um ficheiro .csr designado como "certificate request", recorrendo ao seguinte comando:

```
openssl req -new -key www.virtualhost.pt.key -out  www.virtualhost.pt.csr
```

Será pedida a chave utilizada na criação do ficheiro .key  ao que se seguirá um conjunto de questões utilizadas para a geração do certificate request.

```
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
A challenge password []:
An optional company name []:
```

De salientar que o "common name" deverá ser o seu FQDN exemplificado pelo url **www.virtualhost.pt.**

Após responder às várias questões atrás referidas será criado o ficheiro exemplo **www.virtualhost.csr,** a enviar com o objectivo de obter o certificado final **www.virtualhost pt.crt.**

Para gerar um certificado "self-signed", com a duração por exemplo de um ano, poderá invocar o seguinte comando:

```
openssl x509 -req -days 365 -in www.virtualhost.pt.csr -signkey
www.virtualhost.pt.key -out www.virtualhost.pt.crt
```

Para instalar este certificado deverá actualizar a directiva Apache do seu virtualhost com as seguintes linhas:

```
SSLCertificateFile    /path/to/your/www.virtualhost.pt.crt
SSLCertificateKeyFile /path/to/your/www.virtualhost.pt.key
```

Se tiver realizado o pedido a uma entidade de certificação, ao receber o certificado deverá substituir o certificado gerado temporariamente.

# 10 REFERÊNCIAS

1. SimpleSAMLphp | Feide RnD

   http://rnd.feide.no/simplesamlphp

2. **educause.** *eduperson.* [Online] http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html.

3. Terena, TF-EMC2. SCHAC. [Online]

   http://www.terena.org/activities/tf-emc2/docs/schac/schac-schema-IAD-1.4.0.pdf.