Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

Cookbook – SimpleSAMLphp Identity Provider

Serviço Utilizador RCTS
Janeiro de 2010

11 de Janeiro de 2010

UMIC FCCN Fundação para a Computação Científica Nacional RCTS Financiado por:

Fundação para a Computação Científica Nacional
Foundation for National Scientific Computing

Cookbook – SimpleSAMLphp Identity Provider

Serviço Utilizador RCTS
Janeiro de 2010

EXT/2010/Serviço Utilizador RCTS
Esmeralda Câmara

11 de Janeiro de 2010

ÍNDICE

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 "Identity Provider SimpleSAMLphp" permite realizar a autenticação (LDAP,Mysql,Radius) e comunicar com Shibboleth SP's ou SAML2.0 SP's.

1.1 OBJECTIVOS

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

2 INSTALAÇÃO – SIMPLESAMLPHP SP

2.1 SOFTWARE E PRÉ-REQUISITOS

Antes de dar inicio à instalação e configuração do "Identity 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`. Caso a autenticação seja realizada em LDAP: `ldap`. Autenticação utiliza base de dados são necessários os respectivos drivers: (mysql,pgsql,…).

- ✓ **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 IdP 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 IdP 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 IdP: **idp.key**
- Certificados para o IdP Web Server: **your_idp_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_idp_hostname.pt
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
SSLOptions +StdEnvVars +ExportCertData
SSLCertificateFile /path/to/your/your_idp_hostname.pt.crt
SSLCertificateKeyFile /path/to/your/your_idp_hostname.pt.key
DocumentRoot /home/httpd/your_idp_hostname/html

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

<Directory "/home/httpd/your_idp_hostname.pt/html">
Options Indexes FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
# Logs do Site
ErrorLog /home/httpd/your_idp_hostname/logs/error_log
CustomLog /home/httpd/your_idp_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 IDP - 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

Definir directório base (por omissão é considerado /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

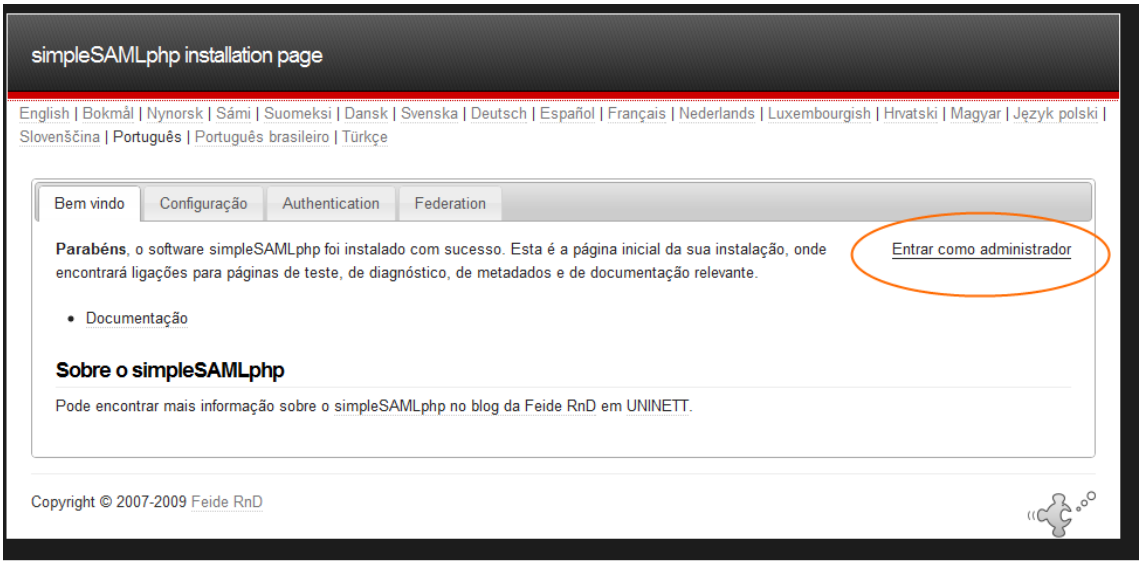
O simpleSAMLphp disponibiliza um interface que permite avaliar a configuração do "Service Provider". Para aceder à zona privada é necessário realizar login com a palavra-chave configurada no ficheiro /var/simplesamlphp/config/config.php.

```
/**
* 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 IdP',
        'technicalcontact_email'    => 'idp_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_idp_hostname.pt/simplesaml**



5.3 ACTIVAR COMPONENTE "IDENTITY PROVIDER"

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

```
/*
         * Enable
         *
         * Which functionality in simpleSAMLphp do you want to enable. Normally
you would enable only
         * one of the functionalities below, but in some cases you could run
multiple functionalities.
         * In example when you are setting up a federation bridge.
         */
        'enable.saml20-idp'             => true,
        'enable.shib13-idp'             => false,
        'enable.wsfed-sp'               => false,

        'enable.authmemcookie' => false,
```

5.4 DIRECTÓRIO DE METADADOS

No directório /var/simplesamlphp/metadados 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 no directório de metadados dependendo do componente que se está a configurar.

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

- ✓ **saml20-idp-hosted.php**

  Se o simpleSAMLphp está activo para a componente "Identity Provider" é neste ficheiro que se identifica o EntityID e respectivos atributos que devem ser enviados para os serviços.

- ✓ **saml20-sp-remote.php**

  Este ficheiro permite configurar os serviços remotos ou seja os "Service Provider's" remotos que pertencem à federação e que podem utilizar o "Identity Provider (identificado no **saml20-idp-hosted.php**) para autenticação e autorização através dos atributos.

No ficheiro de configuração geral é necessário identificar o directório onde o simpleSAMLphp pode encontrar estes ficheiros.

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 os ficheiros saml20-sp-remote.php e saml20-idp-hosted.php nos seguintes directórios:

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

Recomendamos a seguinte configuração:

1. Manter a localização dos ficheiros "hosted" (saml20-idp-hosted.php) no directório de /var/simplesamlphp/metadata.
2. Criar o directório rctsaai em /var/simplesamlphp/metadata e colocar os ficheiros "remote" (saml20-sp-remote.php).

O simpleSAMLphp permite gerar o ficheiro remoto (saml20-sp-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 SIMPLESSAMLPHP IDP - METADADOS DA FEDERAÇÃO

O SimpleSAMLphp permite a actualização periódica de metadados (saml20-sp-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-sp-remote.php com base no link de metadados configurado no modulo.

6.1 MODULO "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_idp_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_idp_hostname.pt/simplesaml/module.php/cron/cron.php?key=SECRET=daily"   >
/dev/null 2>&1
# Run cron [hourly]
01 * * * * curl -k -silent
"https://your_idp_hostname.pt/simplesaml/module.php/cron/cron.php?key=SECRETtag=hourly"
> /dev/null 2>&1
# Run cron [frequent]
XXXXXXXXXX curl -k -silent
"https://your_idp_hostname.pt/simplesaml/module.php/cron/cron.php?key=SECRET&tag=freque
nt" > /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 IDP - AUTENTICAÇÃO

O ficheiro saml20-idp-hosted.php localizado no directório /var/simplesamlphp/metadata é responsável por identificar o entityId do "Identity Provider" e o plugin a utilizar para realizar a autenticação.

A chave do array metadata identifica o **entityId** do IdP : `'https://your_idp_hostname.pt'.`

```
<?php
/*
 * SAML 2.0 Meta data for simpleSAMLphp
 *
 * The SAML 2.0 SP Hosted config is used by the SAML 2.0 SP to identify itself.
 *
 * Required fields:
 *  - host
 *
 * Optional fields:
 *  - NameIDFormat
 *  - ForceAuthn
 *  - redirect.sign
 */

metadata = array(
     'https://your_idp_hostname.pt' => array(
          'host'  => 'your_idp_hostname.pt',
          'certificate' =>'idp.crt',
         // X.509 key and certificate. Relative to the cert directory.
          'privatekey'              =>      'idp.pem',
          // Authentication plugin to use. login.php is the default one that uses LDAP.
          'auth'                            =>      'id_mysql',
        )
);

?>
```

O idp.crt é o certificado utilizado quando é gerada a metadata do IdP. O idp.key é utilizado para assinar as mensagens enviadas para o SP. 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/idp.key /var/simplesamlphp/cert/)

A linha laranja no exemplo acima associa ao Identity Provider o plugin de autenticação 'id_mysql'. Este identificador encontra-se definido no ficheiro

- ✓ ***/var/simplesamlphp/config/authsources.php***

Neste ficheiro é possível definir vários identificadores, em seguida apresentamos exemplos de configuração para o Mysql e LDAP/Active Directory.

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

```
<?php


$config = array(
```

```
    'id_mysql' => array(
          'sqlauth:SQL',
          'dsn' => 'mysql:host=host_bd;port=3306;dbname=nome_da_base_dados',
          'username' => 'utilizador_da_bd',
          'password' => 'password_da_bd',
          'query' => 'SELECT uid,username, mail,givenname,surname,o FROM users WHERE
username = :username AND password = :password',
       ),
```

```
    'id_ldap' => array(
            'ldap:LDAP',
            'hostname'   => 'ldap.example.org',
            'attributes' => null,
            'enable_tls' => false,
            'search.enable' => TRUE,
            'search.base' => 'ou=people,dc=example,dc=org',
            'search.attributes' => array('sAMAccountName'),
            'search.username' => 'cn=administrator,dc=example,dc=org',
            'search.password' => 'password',
    )
);

?>
```

8 SIMPLESAMLPHP IDP - AUTORIZAÇÃO

O Identity Provider deve definir e mapear atributos que devem ser enviados para os serviços. Existem duas configurações distintas dependendo se o serviço faz parte da federação (ex.:moodle-aai) ou se o serviço é externo à federação (ex.: GoogleApps).

8.1 ATRIBUTOS PARA SERVIÇOS DA FEDERAÇÃO

Como referido na secção 6 o módulo metarefresh constrói este ficheiro automaticamente o que leva a que qualquer alteração directa no ficheiro /var/simplesamlphp/metadata/rctsaai/saml20-sp-remote.php fique sem efeito após a execução do metarefresh.

Deste modo o mapeamento de atributos deve realizar-se directamente no ficheiro de configuração do módulo metarefresh.

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

```
<?php


$config = array( 'sets' => array(

        'rctsaai' => array(

        'cron' => array('hourly'),
        'sources'       => array(
              array(

'src' => 'http://metadata-rctsaai.fccn.pt/metadata/RCTSaai_testbedmetadata.xml',
 'template' => array(

 'AttributeNameFormat'   => 'urn:oasis:names:tc:SAML:2.0:attrname-format:uri',
 'authproc' => array(
                        50 => array(
                        'class' => 'core:AttributeMap',
                        'username' => 'urn:oid:2.5.4.3',
                        'mail'=> 'urn:oid:0.9.2342.19200300.100.1.3',
                        'surname' => 'urn:oid:2.5.4.4',
                        'givenname'=> 'urn:oid:2.5.4.42',
                        'o'=>'urn:oid:2.5.4.10')
                        )

                    )
         ),

    ),
   'maxCache' => 60*60*24*4, // Maximum 4 days cache time.
   'maxDuration' => 60*60*24*10, // Maximum 10 days duration on ValidUntil.
    'outputDir' => 'metadata/rctsaai/',
                ),
        ));

?>
```

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.

O exemplo acima é referente ao mapeamento de atributos proveniente do repositório de dados configurado anteriormente (mysql) para o formato "oid". Desta forma todos os serviços que se encontram no ficheiro de metadados da federação quando gerados para o formato php do ficheiro saml20-sp-remote.php tem mapeados estes atributos.

8.2 ATRIBUTOS PARA SERVIÇOS EXTERNOS À FEDERAÇÃO

Os serviços externos à federação têm mapeamento distintos dos utilizados na federação RCTSaai. A solução é criar um segundo ficheiro saml20-sp-remote.php em /var/simplesamlphp/metadata e adicionar a configuração do serviço externo.

Exemplo do Serviço GoogleApps

Ficheiro: /var/simplesamlphp/metadata/saml20-sp-remote.php

```
  /*
   * This example shows an example config that works with Google Apps for education.
   * What is important is that you have an attribute in your IdP that maps to the
local part of the email address
   * at Google Apps. E.g. if your google account is foo.com, and you have a user with
email john@foo.com, then you
   * must set the simplesaml.nameidattribute to be the name of an attribute that for
this user has the value of 'john'.
   */
  'google.com' => array(
    'AssertionConsumerService'   => 'https://www.google.com/a/g.feide.no/acs',
    'spNameQualifier'            => 'google.com',
    'NameIDFormat'                          =>  'urn:oasis:names:tc:SAML:2.0:nameid-
format:email',
    'simplesaml.nameidattribute' => 'uid',
    'simplesaml.attributes'      => false
  );
```

O simpleSAMLphp realiza o "merge" de ambos os ficheiros saml20-sp-remote.php desde que a localização de metadata.sources no ficheiro de configuração geral esteja de acordo com a configuração da secção 5.4 deste documento.

8.3 METADADOS DO IDENTITY PROVIDER

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

- **https://<your_idp_hostname>/simplesaml/saml2/idp/metadata.php**

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

9 PONTOS DE CONTACTO

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

10 ANEXOS

10.1 CRIAR CERTIFICADO SSL

```
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.

11 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.