

Shibboleth SP 3.0 - Install&Configure

Konfigurace pro potřeby federace cvutID na serveru "pepa" s operačním systémem Debian 10.0 a webovým serverem Apache2 s podporou SSL - podrobnější a obecnější návod můžete nalézt na stránkách České akademické federace identit eduID.cz.

Instalace balíčku shibboleth

install

```
# Instalace Shibboleth SP vetn modul pro Apache HTTP server
apt-get install libapache2-mod-shib
# Varianta pro CentOS7
curl --output /etc/yum.repos.d/security:shibboleth.repo http://download.opensuse.org/repositories/security:/shibboleth/CentOS_7/security:shibboleth.repo
yum install shibboleth.x86_64
```

Konfigurace předpokládá již nainstalované balíčky apache2 a shibboleth.

Instalace OpenSSL certifikátů

Přes osoby na fakultách ČVUT [pověřené](#) vygenerujte serverový certifikát a klíč, který umístíte na server do /etc/ssl.

Konfigurace web serveru - Apache2

V již nainstalovaném Apache serveru s modulem SSL provedete několik změn v souboru /etc/apache2/sites-enabled/default-ssl.

- Přesměrujte odkaz na metadata serveru (pak pošlete tento odkaz správci IdP, aby Vás mohl zaregistrovat do metadat federace cvutID).
- Zkontrolujte cesty k OpenSSL certifikátům /etc/ssl.
- Vytvoříte složku pro aplikaci např.: /var/www/secure a povolíte nad ní autentizaci přes modul shibboleth (modul zapnete příkazem a2en mod shib nebo vložíte do konfigurace direktivu LoadModule mod_shib /usr/lib/shibboleth/mod_shib2.so).

/etc/apache2/sites-enabled/default-ssl

```
Redirect seeother /shibboleth https://pepa.cvut.cz/Shibboleth.sso/Metadata

SSLCertificateFile /etc/ssl/certs/pepa.cvut.cz.pem.crt
SSLCertificateKeyFile /etc/ssl/private/pepa.cvut.cz.pem.key
SSLCertificateChainFile /etc/ssl/certs/tcs-ca-bundle.pem

<Location /secure>
    AuthType          shibboleth
    Require            shibboleth
    ShibRequestSetting requireSession 1
</Location>
```

Konfigurace SP - shibboleth2.xml

Provedte několik změn v souboru /etc/shibboleth/shibboleth2.xml

- Vyplňte jméno serveru/aplikace "entityID".
- Nastavte "session" na 8 hodin (28800 sekund) a "timeout" na 1 hodinu.
- Nastavte poskytovatele identity (IdP) pro cvutID.
- Vyberte zdroj pro stahování metadat cvutID. Metadata se pak budou zalohovat do /var/cache/shibboleth/cvutid-metadata.xml.
- Zkontrolujte cestu k OpenSSL certifikátům /etc/shibboleth/ a nastavte přístup pro shibd demona chown _shibd pepa.cvut.cz.*

/etc/shibboleth/shibboleth2.xml

```
<ApplicationDefaults entityID="https://pepa.cvut.cz/shibboleth"
    REMOTE_USER="uid eppn persistent-id targeted-id">

<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
    checkAddress="false" handlerSSL="true" cookieProps="https">

#discoveryURL or single entityID see in example
<SSO entityID="https://idp2.civ.cvut.cz/idp/shibboleth">
    SAML2
</SSO>

#MetadataProvider type="Chaining" or single type="XML" see in example
<MetadataProvider type="XML" validate="true"
    url="https://idp2.civ.cvut.cz/cvutid/cvutid-metadata.xml"
    backingFilePath="cvutid-metadata.xml" maxRefreshDelay="900">
</MetadataProvider>

<CredentialResolver type="File" key="sp-key.pem" certificate="sp-cert.pem"/>
```

Pro zjednodušení výměny metadat jsme začali podporovat self-sign certifikáty s dobou platnosti 10 let a více. Certifikát a klíč vygenerujete příkazem:

```
shib-keygen -h pepa.cvut.cz -y 10 -e https://pepa.cvut.cz/shibboleth
```

Významy přepínačů jsou -h jméno serveru, -y doba platnosti, -e entityID. Klíč a certifikát (sp-cert.pem a sp-key.pem) se Vám uloží do složky /etc/shibboleth.

Příklad konfigurace pro přístup k více IdP serverům z federace eduID.cz přes WAYF (WhereAreYouFrom) nebo DS (Discovery Service) s použitím filtru pro ČVUT a VŠCHT. V souboru /etc/shibboleth/shibboleth2.xml provedeme dvě změny.

/etc/shibboleth/shibboleth2.xml

```
#discoveryURL or single entityID see in example
<SSO discoveryProtocol="SAMLDS"
    discoveryURL="https://ds.eduid.cz/wayf.php?
filter=eyJhbGxvd0ZlZWxzIjogWyJlZHVJRC5jeiJdLCAiYWxsY3dJZFZBZSIjogWyJodHRwczovL3dzc28udnNjaHQuY3ovaWRwL3NoaWJib2xldGgiLCJodHRwczovL2lkcdiUy212LmN2dXQuY3ovaWRwL3NoaWJib2xldGgiXSwgImFsbG93SG9zdGVsIjogZmFsc2UsICJhbGxvd0hvc3RlbFJlZyI6IGZhbHNlfQ=="&lang="cz">
    SAML2 SAML1
</SSO>

#MetadataProvider type="Chaining" or single type="XML" see in example
<MetadataProvider type="Chaining">
    <MetadataProvider type="XML" path="/etc/shibboleth/vschtid-metadata.xml"/>
    <MetadataProvider type="XML" url="https://idp2.civ.cvut.cz/cvutid/cvutid-metadata.xml"
backingFilePath="/etc/shibboleth/cvutid-metadata.xml" reloadInterval="3600"/>
</MetadataProvider>
```

Generátor filtru naleznete na stránkách eduid.cz.

Konfigurace SP - attribute-map.xml

Stáhněte si aktuální soubor [attribute-map.xml](#) se všemi atributy poskytoványými ve federaci cvutID a nahraďte jím soubor původní /etc/shibboleth/attribute-map.xml.

Otestování konfigurace

Pro otestování konfigurace vložte do složky secure/ php script `index.php`, který slouží k vypsání všech atributů daného uživatele. Po zadání adresy `https://jméno_serveru/secure/index.php` do prohlížeče, budete přesměrováni na IdP, kde zadáte jméno a heslo z usermap.cvut.cz. Pokud bude dotaz úspěšný, zobrazí se Vám všechny atributy přihlášeného uživatele. Výpis atributů by měl být shodný jako na testovacím serveru [tps://oliva.civ.cvut.cz](https://oliva.civ.cvut.cz) jiný výpis atributů naleznete na serveru <https://attributes.eduid.cz>.

/var/www/secure/index.php

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="cs">
<head>
<title>the Test Page of cvutID</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<body><pre>
<?php print_r($_SERVER); ?>
</pre></body>
</html>
```

...a je to 😊

Snad ještě příklad v jazyce [JAVA](#).