SAML u PHP aplikacijama

U sustavu AAI@EduHr za implementaciju SSO autentikacijskog modula u PHP aplikacijama koristi se programski alat SimpleSAMLphp. Navedeni programski alat može se instalirati iz Debian paketa ili ručno, raspakiravanjem arhive koja sadrži programski alat SimpleSAMLphp prilagođen sustavu AAI@EduHr u odgovarajući direktorij dostupan web poslužitelju.

Za primjenu u sustavu AAI@EduHr dostupna je verzija: SimpleSAMLphp 1.19.7 Ako to produkcijska okolina dopušta, uvijek je poželjno instalirati najnoviju verziju.

Starije verzije programskog alata SimpleSAMLphp više nisu podržane od strane AAI@EduHr tima.

Instalacija programskog alata SimpleSAMLphp

Programski alat SimpleSAMLphp prilagođen za autentikaciju putem sustava AAI@EduHr možete raspakirati iz arhive simplesamlphp-aai-1.19.7.tar.gz ili iz odgovarajućeg **simplesamlphp-aai** Debian paketa (prilikom instalacije iz paketa obratite pozornost da nije dovoljno instalirati paket **simplesamlphp**, već je potrebno instalirati i paket **simplesamlphp-aai**).

U nastavku uputa podrazumjevat ćemo da ste neku od gore navedenih arhiva raspakirali u direktorij **/var/www/**. Ako ste SimpleSAMLphp instalirali u neki drugi direktorij, u daljnim uputama jednostavno zamijenite direktorij **/var/www/** direktorijem u kojem ste instalirali SimpleSAMLphp. Nakon raspakiravanja arhive potrebno je napraviti sljedeće:

- kreirajte simbolički link:

```
ln -s /var/www/simplesamlphp-aai-1.19.7 /var/www/simplesamlphp
```

- u datoteci:

```
/var/www/simplesamlphp/config/config.php
```

postavite odgovarajuće vrijednosti parametara 'auth.adminpassword', 'technicalcontact_name', 'technicalcontact_email' i 'secretsalt'

- U istoj datoteci inicijalno su podešene opcije **session.cookie.samesite' => 'None'** i **'session.cookie.secure' => true** kako bi vaša instanca simplesamlphp-a podesila SameSIte kolačić u None. Više o SameSite kolačiću pročitajte ovdje. Ako ne želite slati SameSite kolačić (oprez!) postavite opciju **session.cookie.samesite' => false.** Naša je preporuka koristiti isključivo https protokol. Ako ipak koristite i http, možete isključiti i opciju **'session.cookie.secure'**
- U odgovarajućoj konfiguracijskoj datoteci Apache poslužitelja (standardno **httpd.conf**) za vaš web dodajte liniju:

```
Alias /simplesaml /var/www/simplesamlphp/www
```

i nakon toga učitajte novu konfiguraciju Apache poslužitelja ili jednostavno restartajte poslužitelj.

Napredno konfiguriranje SimpleSAMLphp autentikacijskog modula

U većini slučajeva SimpleSAMLphp autentikacijski modul instaliran prema gore navedenim uputama trebao bi funkcionirati ispravno. Međutim, u određenim uvjetima dobro je podesiti još neke parametre.

Dnevnički zapisi

Standardno, SimpleSAMLphp je iskonfiguriran da dnevničke zapise piše u **syslog**. Ako radi bolje preglednosti želite da se dnevnički zapisi zapisuju u datoteku **simplesamlphp.log**, trebate podesiti da Apache ima dozvolu pisanja u navedenu datoteku:

```
chown root:apache /var/www/simplesamlphp/log/simplesamlphp.log
chmod 620 /var/www/simplesamlphp/log/simplesamlphp.log
```

Također, SimpleSAMLphp standardno koristi **PHP session** za pohranu session varijabli. Da bi se izbjegao potencijalni konflikt prilikom pohrane varijabli između PHP aplikacije i programskog alata SimpleSAMLphp, SimpleSAMLphp se može iskonfigurirati tako da varijable pohranjuje u **SQLite bazu** ili u **Memcache**.

Podešavanje pisanja session varijabli u SQLite

Potrebno je omogućiti Apache poslužitelju da čita i piše u direktorij **../data/** unutar programskog alata SimpleSAMLphp:

```
chown root:apache /var/www/simplesamlphp/data/
chmod 770 /var/www/simplesamlphp/data/
```

i nakon toga u konfiguracijskoj datoteci **/var/www/simplesamlphp/config/config.php** podesiti sljedeće parametre:

```
'store.type' => 'sql',
'store.sql.dsn' => 'sqlite:/var/www/simplesamlphp/data/sqlitedatabase.sq3',
```

Na taj način, SimpleSAMLphp će svoje varijable pohranjivati u SQLite datoteku **/var/www/simplesamlphp/data/sqlitedatabase.sq3** i PHP aplikacija ih neće 'pregaziti'.

Podešavanje pisanja session varijabli u Memcache

Na poslužitelju mora biti instaliran i pokrenut memcache.

U konfiguracijskoj datoteci **/var/www/simplesamlphp/config/config.php** podesiti parametar:

```
 'store.type' => 'memcache',
```

Registracija novog resursa u sustavu AAI@EduHr

Da bi autentikacija kroz sustav AAI@EduHr bila omogućena, potrebno je zatražiti registraciju novog resursa u sustavu AAI@EduHr prema uputama na stranici Registar resursa.

Parametre koje je prilikom registracije resursa potrebno upisati u odjeljku SAML metapodaci možete saznati na način da se web preglednikom prijavite u sučelje za administratore programskog alata SimpleSAMLphp koje bi se, ovisno o nazivu poslužitelja, trebalo nalaziti na adresi:

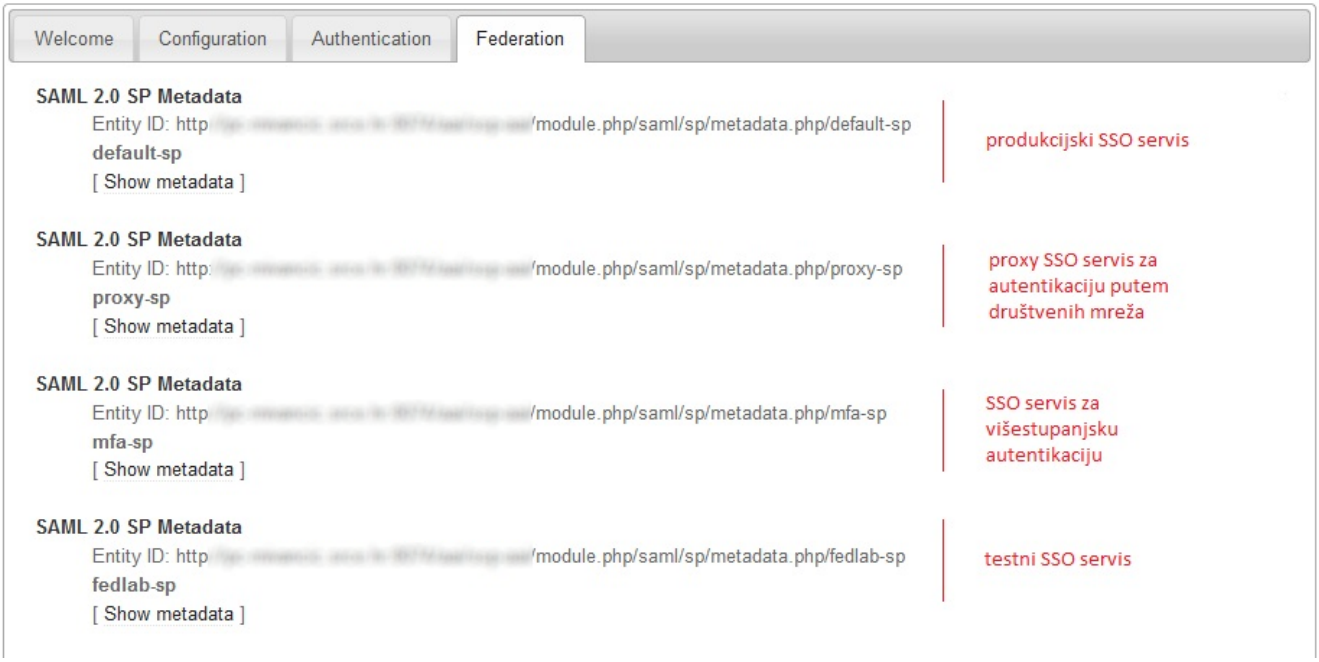
`http(s)://fqdn_naziv_posluzitelja/simplesaml/`

Ako ste SimpleSAMLphp instalirali iz paketa, zaporku za prijavu u administratorsko sučelje možete pronaći u datoteci:

`/var/lib/simplesamlphp/secrets.inc.php`

Ako ste SimpleSAMLphp instalirali ručno, zaporka za prijavu u administratorsko sučelje zapisana je kao vrijednost parametra 'auth.adminpassword' u datoteci /var/www/simplesamlphp/config/config.php

Nakon što se prijavite u administratorsko sučelje, kliknite na karticu Federacija (engl. Federation). Otvorit će vam se sučelje kao na sljedećoj slici:



s nekoliko odjeljaka u kojima su definirani metapodaci ovisno o tome koji autentikacijski servis vaša aplikacija treba koristiti:

- **default-sp** - metapodaci koji opisuju vašu aplikaciju u slučaju da za autentikaciju koristite produkcijski AAI@EduHr SSO servis;
- **proxy-sp** - metapodaci koji opisuju vašu aplikaciju u slučaju da za autentikaciju želite koristiti društvene mreže;
- **mfa-sp** - metapodaci koji opisuju vašu aplikaciju u slučaju da za autentikaciju želite koristiti SSO servis za višestupanjsku autentikaciju;
- **fedlab-sp** - metapodaci koji opisuju vašu aplikaciju u slučaju da za autentikaciju koristite testni SSO servis;

Za svaku grupu metapodataka navedena je vrijednost parametra **Entity ID** kojeg treba unijeti u polje **Jedinstveni identifikator resursa** prilikom postavljanja zahtjeva za registracijom novog resursa.

Klikom na opciju **Prikaži metapodatke** (engl. Show Metadata) otvorit će vam se stranica s prikazom metapodataka u XML i SimpleSAMLphp formatu na kojoj možete pronaći vrijednosti preostalih dvaju parametara (**AssertionConsumerService URL** i **SingleLogoutService URL**) koje je potrebno unijeti prilikom popunjavanja zahtjeva za registracijom novog resursa:

Metapodaci

Metapodaci u SAML 2.0 XML formatu:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://developer.aaiedu.hr/ssp/module.ph
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:prot
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://developer.aai
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://developer.aa
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post" Location="http://developer
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="http://develope
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01" Location="http://developer.
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:profiles:holder-of-key:SSO:browser" Location="htt
  </md:SPSSODescriptor>
  <md:ContactPerson contactType="technical">
    <md:GivenName>Kontakt</md:GivenName>
    <md:SurName>Osoba</md:SurName>
    <md:EmailAddress>kontakt.osoba@ustanova.hr</md:EmailAddress>
  </md:ContactPerson>
</md:EntityDescriptor>
```

U simpleSAMLphp formatu - koristite ovu opciju ako se na drugoj strani također nalazi simpleSAMLphp entitet:

```
$metadata['http://developer.aaiedu.hr/ssp/module.php/saml/sp/metadata.php/fedlab-sp'] = array (
  'AssertionConsumerService' => 'http://developer.aaiedu.hr/ssp/module.php/saml/sp/saml2-acs.php/fedlab-sp',
  'SingleLogoutService' => 'http://developer.aaiedu.hr/ssp/module.php/saml/sp/saml2-logout.php/fedlab-sp',
);
```

Obzirom da većina novoregistriranih resursa najprije treba proći kroz fazu razvoja i testiranja, prilikom registracije novog resursa najprije je u registru potrebno unijeti metapodatke za testni SSO servis, odnosno **fedlab-sp** metapodatke.

Kada servis bude spreman za produkciju, u registru resursa je potrebno ažurirati SAML metapodatke na način da se podaci za testni SSO servis zamijene podacima koji odgovaraju produkcijskom SSO servisu, odnosno **default-sp** metapodacima.

Metapodaci za **proxy-sp** odnose se na servis koji, osim autentikacije korisnika putem sustava AAI@EduHr, omogućuje i autentikaciju korisnika putem vanjskih autentikacijskih servisa (npr. društvenih mreža). Prilikom korištenja ovog autentikacijskog mehanizma treba voditi pažnju da se skup atributa koji će biti vraćen kao odgovor za svaki pojedini vanjski autentikacijski servis razlikuje, te se prenose svi atributi koji su dostupni.

Metapodaci za **mfa-sp** odnose se na servis koji uz autentikaciju korisnika putem sustava AAI@EduHr omogućuje i autentikaciju korisnika dodatnim mehanizmom, npr. pomoću sustava za generiranje jednokratnih tokena. Detaljnije upute za postavljanje višestupanjske konfiguracije dostupne su na poveznici Registar resursa#SAMLkonfiguracijazavi%C5%A1estupanjskuautentikaciju.

Automatsko osvježavanje IdP metapodataka

SimpleSAMLphp dostupan u ovim uputama unaprijed je konfiguriran sa IdP (eng. Identity Provider) metapodacima sustava AAI@EduHr. U nekim slučajevima, te metapodatke je potrebno osvježiti, tipično zbog promjene certifikata kojim se može provjeravati potpis u SAML porukama. Ako želite omogućiti automatsko osvježavanje metapodataka, možete učiniti sljedeće:

* omogućite module 'cron' i 'metarefresh':

```
touch /var/www/simplesamlphp/modules/cron/enable
touch /var/www/simplesamlphp/modules/metarefresh/enable
```

* osigurajte da web server može pisati u direktorij ../**metadata**, odnosno da može pisati u datoteku metadata/saml20-idp-remote.php, npr:

```
chown -R root:apache /var/www/simplesamlphp/metadata/
chmod -R 770 /var/www/simplesamlphp/metadata/
```

* u datoteci ../**config/module_cron.php** promijenite vrijednost 'tajni-random-string' za ključ 'key' u vrijednost sa slučajnim nizom znakova (vrijednost ne bi trebalo biti moguće lako pogoditi)

* pripremljena konfiguracija očekuje pokretanje cron-a svakih sat vremena, pa postavite cron kao u primjeru ispod (prilagodite vrijednost za parametar 'key' prema konfiguraciji u datoteci ../**config/module_cron.php**):

```
# Run cron: [hourly]
01 * * * * curl --silent "http(s)://fqdn_naziv_posluzitelja/simplesaml/module.php/cron/cron.php?key=tajni-random-string&tag=hourly" > /dev/null 2>&1
```

Primjer korištenja

Primjere PHP skripti **index.php** i **logout.php** koje demonstriraju uporabu programskog alata SimpleSAMLphp za prijavu i odjavu korisnika možete pronaći u authdemo arhivi.

Ovisno o tome gdje je na vašem poslužitelju instaliran SimpleSAMLphp, na početku obje skripte unutar naredbe **require_once()** trebate postaviti odgovarajuću putanju do skripte **_autoload.php**. Primjerice, ako ste SimpleSAMLphp instalirali iz paketa, ispravna putanja trebala bi biti:

```
require_once('/usr/share/simplesamlphp/lib/_autoload.php');
```

Analogno, ako ste SimpleSAMLphp instalirali ručno (npr. u direktorij **/var/www/**), trebate navesti putanju sukladno direktoriju u kojem ste instalirali SimpleSAMLphp:

```
require_once('/var/www/simplesamlphp/lib/_autoload.php');
```

Bitno je naglasiti da je u skriptama standardno postavljeno da se autentikacija vrši putem `testnog autentikacijskog servisa` namijenjenog aplikacijama koje se nalaze u fazi razvoja i testiranja jer se podrazumijeva da sve nove aplikacije koje žele koristiti sustav AAI@EduHr za autentikaciju korisnika najprije trebaju proći kroz fazu testiranja.

Obzirom da se u testnom okruženju iz sigurnosnih razloga ne mogu koristiti produkcijski AAI@EduHr elektronički identiteti, kreiranje testnih elektroničkih identiteta možete zatražiti putem web forme na adresi:

https://fed-lab.aaiedu.hr/zahtjev.php?show=zahtjev_identitet

Nakon što aplikacija prođe kroz fazu razvoja i testiranja, u produkcijsko AAI@EduHr okruženje ju možete uključiti na način da u skriptama za prijavu i odjavu korisnika liniju

```
$as = new SimpleSAML_Auth_Simple('fedlab-sp');
```

zamijenite linijom

```
$as = new SimpleSAML_Auth_Simple('default-sp');
```

te putem `Registra resursa` zatražite promjenu statusa resursa iz test u produkcija.

Za sve dodatne informacije, rješavanje problema i bilo kakvih eventualnih nejasnoća kontaktirajte nas elektroničkom poštom na `aai@srce.hr`

Važna napomena (samo za Debian Linux)

Da bi autentikacija i razmjena podataka ispravno funkcionirala na poslužiteljima s Debian Linux operacijskim sustavom, nakon instalacije SimpleSAMLphp-a potrebno je postaviti vrijednost Suhosin parametra:

```
suhosin.get.max_value_length = 16382
```

Ako se instalacija vrši iz paketa **simplesamlphp-aai**, ova vrijednost će biti automatski postavljena. U suprotnom je odgovarajuću vrijednost navedenog Suhosin parametra potrebno postaviti ručno.