Upute za korištenje AAI@EduHr Laba

AAI@EduHr Lab funkcionira na gotovo identičan način kao i produkcijski SSO servis s tom razlikom što se u AAI@EduHr Lab okruženju mogu koristiti isključivo testni elektronički identiteti. Za korištenje AAI@EduHr Lab usluge potrebno je registrirati resurs na sličan način na koji se registriraju i produkcijski resursi u sustavu AAI@EduHr.

0) Testni elektronički identiteti

U AAI@EduHr Labu moguće je koristiti isključivo testne elektroničke identitete. Ako već ne posjedujete testni elektronički identitet, morate ga kreirati (bez njega nećete moći testirati autentikaciju u testnom okruženju).

Testni e-identitet u LDAP imenuku s domenom *aai-test.hr* možete zahtjevati putem obrasca dostupnog ovdje.

U slučaju potrebe, zaseban testni LDAP imenik s domenom po izboru možete zahtijevati putem obrasca dostupnog ovdje. U zasebnom testnom LDAP imeniku sami kreirate testne elektroničke identitete po potrebi.

1) Proces registracije resursa

Procedura za registraciju testnog resursa gotovo je identična proceduri za registraciju produkcijskog resursa, razlika je samo u vrijednosti parametra Vrsta resursa. Za registraciju testnog resursa potrebno je prijaviti se u online Registar resursa, odabrati opciju Registracija resursa, popuniti formu s općim podacima o resursu i SAML metapodacima te poslati zahtjev za registraciju. Pritom je važno naglasiti da u formi za registraciju resursa, u polju Vrsta resursa treba biti postavljena vrijednost *Test*.

Nakon što zahtjev za registraciju resursa odobri AAI@EduHr tim, autentikacija putem AAI@EduHr Lab Single Sign-On servisa bit će omogućena, a osoba koja je postavila zahtjev za registraciju dobit će o tome obavijest elektroničkom poštom.

Važne napomene

1. Iz sigurnosnih razloga pristup AAI@EduHr registru resursa omogućen je samo korisnicima čiji zahtjev za prijavu u Registar odobri Koordinator sustava AAI@EduHr (Srce). Stoga je prilikom inicijalne prijave u Registar potrebno navesti razlog zbog kojeg biste trebali imati mogućnost korištenja Registra resursa.

2. Ako prvi put registrirate neki resurs putem AAI@EduHr registra resursa ili do sada niste imali nikakvih iskustava s autentikacijskim protokolima, moguće je da nećete znati popuniti pojedina polja prilikom registracije resursa. U slučaju da imate bilo kakvih problema s popunjavanjem forme za registraciju resursa, kontaktirajte AAI@EduHr razvojni tim.

2) Metapodaci autentikacijskog servisa i protokoli

Obzirom da resursi koji imaju status *Test* ne mogu koristiti produkcijsku inačicu sustava jedinstvene autentikacije korisnika, u konfiguraciji klijenta potrebno je unijeti parametre po određenom autentikacijskom protokolu za pristup određenoj inačici sustava jedinstvene autentikacije korisnika implementiranoj u sklopu AAI@EduHr Lab-a.

Metapodaci SSO instanci u testnom okruženju dostupni su preko sljedećih poveznica:

- instanca 'sso': https://fed-lab.aaiedu.hr/sso/saml2/idp/metadata.php?output=xhtml
- instanca 'shib': https://fed-lab.aaiedu.hr/shib/saml2/idp/metadata.php?output=xhtml
- instanca 'ms': https://fed-lab.aaiedu.hr/ms/saml2/idp/metadata.php?output=xhtml

U nastavku su navedene upute na koji način se najčešće klijenti (autentikacijski moduli) podešavaju za autentikaciju putem razvojnog sustava jedinstvene autentikacije.

Važna napomena

Ako je programska podrška na vašem poslužitelju već bila iskonfigurirana za korištenje produkcijskog AAI@EduHr Single Sign-On servisa, prije nego što krenete raditi izmjene navedene u nastavku napravite kopiju svake datoteke u kojoj radite izmjene kako biste u trenutku eventualne promjene statusa resursa iz testnog u produkcijski mogli što lakše vratiti konfiguraciju podešenu za uporabu produkcijskog Single Sign-On servisa.

SAML postavke

simpleSAMLphp (PHP):

Ako se kao autentikacijski modul koristi SimpleSAMLphp, datoteka **../metadata/saml20-idp-remote.php** treba sadržavati metapodatke AAI@EduHr Lab-a (vrijednost za 'certData' potrebno je kopirati iz metapodataka https://fed-lab.aaiedu.hr/sso/saml2/idp/metadata.php?output=xhtml):

```
$metadata['https://fed-lab.aaiedu.hr/sso/saml2/idp/metadata.php'] = array (
  'metadata-set' => 'saml20-idp-remote',
  'entityid' => 'https://fed-lab.aaiedu.hr/sso/saml2/idp/metadata.php',
  'SingleSignOnService' => 'https://fed-lab.aaiedu.hr/sso/saml2/idp/SSOService.php',
  'SingleLogoutService' => 'https://fed-lab.aaiedu.hr/sso/saml2/idp/SingleLogoutService.php',
  'certData' => '...string-vrijednost-x509-certifikata...',
);
```

Inače, uz standardni XML, na poveznici https://fed-lab.aaiedu.hr/sso/saml2/idp/metadata.php?output=xhtml se nalazi i unaprijed pripljemljen PHP kod za SimpleSAMLphp koji predstavlja metapodatke SSO Lab instance, pa ga od tamo možete jednostavno kopirati.

Dalje, u datoteci **../config/authsources.php**, u segmentu koji se odnosi na *Service Provider* parametar kojeg koristi vaša aplikacija (standardno je to **default-sp**, ali za autentikaciju preko fed-lab.aaiedu.hr servisa trebate koristiti **fedlab-sp**) varijabla **idp** treba sadržavati vrijednost kao što je prikazano u nastavku:

```
'fedlab-sp' => array(
  'saml:SP',
  'entityID' => NULL,
  'idp' => 'https://fed-lab.aaiedu.hr/sso/saml2/idp/metadata.php',
  'discoURL' => NULL,
),
```

Napomena: Prethodno navedene upute trebale bi vrijediti za sve inačice programskog alata SimpleSAMLphp počevši od verzije 1.5 nadalje. Međutim, zbog sigurnosnih razloga preporučamo verziju koja je inače dostupna u uputama za implementaciju autentikacije u PHP aplikacijama.

Shibboleth (Java):

Ako se kao autentikacijski modul koristi Shibboleth 2.x, u datoteci **metadata.xml**, unutar taga **EntityDescriptor** treba postaviti slijedeće vrijednosti parametra **validUntil** i **entityID**:

```
validUntil="2023-05-17T00:00:00Z"
entityID="https://fed-lab.aaiedu.hr/shib/saml2/idp/metadata.php"
```

Vrijednost parametra **validUntil** označava do kada vrijede podaci navedeni u datoteci **metadata.xml**. Obzirom da se ti podaci u pravilu ne mijenjaju često, u pravilu se taj datum poklapa s datumom isteka aktualnog certifikata kojim SSO servis potpisuje autentikacijske odgovore.

Zatim je u bloku **<IDPSSODescriptor> ... </IDPSSODescriptor>** u odjeljku:

```
<KeyDescriptor use="signing">
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
...
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
```

između tagova **<ds:X509Certificate>** i **</ds:X509Certificate>** umjesto postojećeg potrebno ubaciti certifikat koji se nalazi na adresi

https://fed-lab.aaiedu.hr/shib/module.php/saml/idp/certs.php/idp.crt

Napomena: Prilikom kopiranja sadržaja certifikata NE SMIJE se iskopirati prva (BEGIN CERTIFICATE) i zadnja (END CERTIFICATE) linija, nego samo ono što se nalazi između njih.

Također, pri samom kraju bloka **<IDPSSODescriptor> ... </IDPSSODescriptor>** potrebno je navesti adresu **AssertionConsumer** servisa:

```
<SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://fed-lab.
aaiedu.hr/shib/saml2/idp/SSOService.php"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://fed-lab.
aaiedu.hr/shib/saml2/idp/SSOService.php"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://fed-lab.
aaiedu.hr/shib/saml2/idp/SSOService.php"/>
```

Time su završene sve potrebne izmjene u datoteci **metadata.xml**.

U datoteci **shibboleth2.xml** u bloku **<SessionInitiator type="Chaining" ... > </SessionInitiator>** postojeću vrijednost parametra **entityID** treba zamijeniti sljedećom vrijednošću:

```
entityID="https://fed-lab.aaiedu.hr/shib/saml2/idp/metadata.php"
```

Na kraju, da bi se učitala nova konfiguracija potrebno je **restartati Shibboleth servis**.

OIOSAML.NET (Microsoft .NET platforma)

Ako se kao autentikacijski modul koristi OIOSAML.NET, za autentikaciju putem AAI@EduHr Lab Single Sign-On servisa vrijede upute na stranici Implementacija autentikacije putem sustava AAI@EduHr u .NET web aplikacijama uz nekoliko manjih izmjena:

U koraku 10 blok **<IDPEndPoints metadata="C:\metadata\>...</IDPEndPoints>** treba imati sljedeći sadržaj:

```
<IDPEndPoints metadata="C:\metadata\>
<add id="https://fed-lab.aaiedu.hr/ms/saml2/idp/metadata.php">
<CertificateValidation>
<add type="dk.nita.saml20.Specification.SelfIssuedCertificateSpecification, dk.nita.saml20"/>
</CertificateValidation>
</add>
</IDPEndPoints>
```

U koraku 10 metapodatke treba dohvatiti s adrese https://fed-lab.aaiedu.hr/ms/saml2/idp/metadata.php

CAS postavke

Za testno okruženje, CAS klijent je potrebno postaviti na sljedeći način:

CAS Server Hostname: fed-lab.aaiedu.hr
CAS Server Port: 443
CAS Server Context: /sso/module.php/casserver
CAS CA Cert Path: https://fed-lab.aaiedu.hr/sso/module.php/saml/idp/certs.php/idp.crt
CAS Login: https://fed-lab.aaiedu.hr:443/sso/module.php/casserver/login
CAS Logout: https://fed-lab.aaiedu.hr:443/sso/module.php/casserver/logout
CAS Service Validate: https://fed-lab.aaiedu.hr:443/sso/module.php/casserver/serviceValidate

OIDC postavke

Za testno okruženje, prilikom konfiguriranja OIDC klijenta, umjesto produkcijskog potrebno je koristiti AAI@EduHr Lab OIDC konfiguracijski URL: https://fed-lab.aaiedu.hr/.well-known/openid-configuration.

3) Migracija iz testnog u produkcijsko okruženje

Od uvođenja AAI@EduHr Lab Single Sign-On servisa u produkciju, resursi koji koriste AAI@EduHr sustav jedinstvene autentikacije fizički su razdvojeni u dvije skupine:

- Resursima koji u Registru resursa kao vrijednost parametra **Vrsta resursa** imaju postavljeno **Test** omogućena je autentikacija isključivo putem **testnog AAI@EduHr Single Sign-On servisa** uz uporabu elektroničkih identiteta pohranjenih u testnim LDAP imenicima kreiranim u sklopu AAI@EduHr Lab-a.
- Resursima koji u Registru resursa kao vrijednost parametra **Vrsta resursa** imaju postavljeno **Produkcija** omogućena je autentikacija isključivo putem **produkcijskog AAI@EduHr Single Sign-On servisa** uz uporabu elektroničkih identiteta pohranjenih u LDAP imenicima matičnih ustanova u sustavu AAI@EduHr.

Niti jedan resurs ne može istodobno imati pristup i testnom i produkcijskom Single Sign-On servisu.

Ovisno o tehnologiji, programskom jeziku i autentikacijskom protokolu korištenom za implementaciju pojedinog resursa, za pristup **produkcijskom** AAI@EduHr Single Sign-On servisu potrebno je na strani resursa iskonfigurirati parametre u skladu sa standarnim uputama za pojedini autentikacijski protokol.

Za pristup **testnoj** inačici Single Sign-On servisa potrebno je slijediti iste upute kao i kod produkcijskog servisa i nakon toga još napraviti izmjene opisane u koraku 2) na ovoj stranici.

Prilikom migracije resursa iz testnog u produkcijsko okruženje (i obrnuto), na strani AAI@EduHr sustava potrebno je u Registru resursa promijeniti vrijednost polja **Vrsta resursa** i kliknuti na opciju **Zatraži promjenu podataka**. Na taj način ćete postaviti zahtjev za promjenu statusa resursa. Prilikom prebacivanja resursa iz testnog u produkcijsko okruženje, zahtjev za promjenom najprije treba odobriti odgovorna osoba matične ustanove s kojom je resurs povezan, a potom i netko od administratora sustava AAI@EduHr. Nakon što administrator sustava AAI@EduHr odobri zahtjev za izmjenom statusa, ovisno o vrsti zahtjeva resurs će biti prebačen iz konfiguracije testnog u konfiguraciju produkcijskog AAI@EduHr Single Sign-On servisa ili obrnuto.

Za sva dodatna pitanja i pomoć pri rješavanju eventualnih problema možete kontaktirati administratore sustava AAI@EduHr slanjem elektroničke pošte na adresu aai@srce.hr.