



SSO

Single Sign On

Sistem enotne prijave

Keywords:

Enotno uporabniško ime

IdP

Shibboleth

Enotna prijava

SP

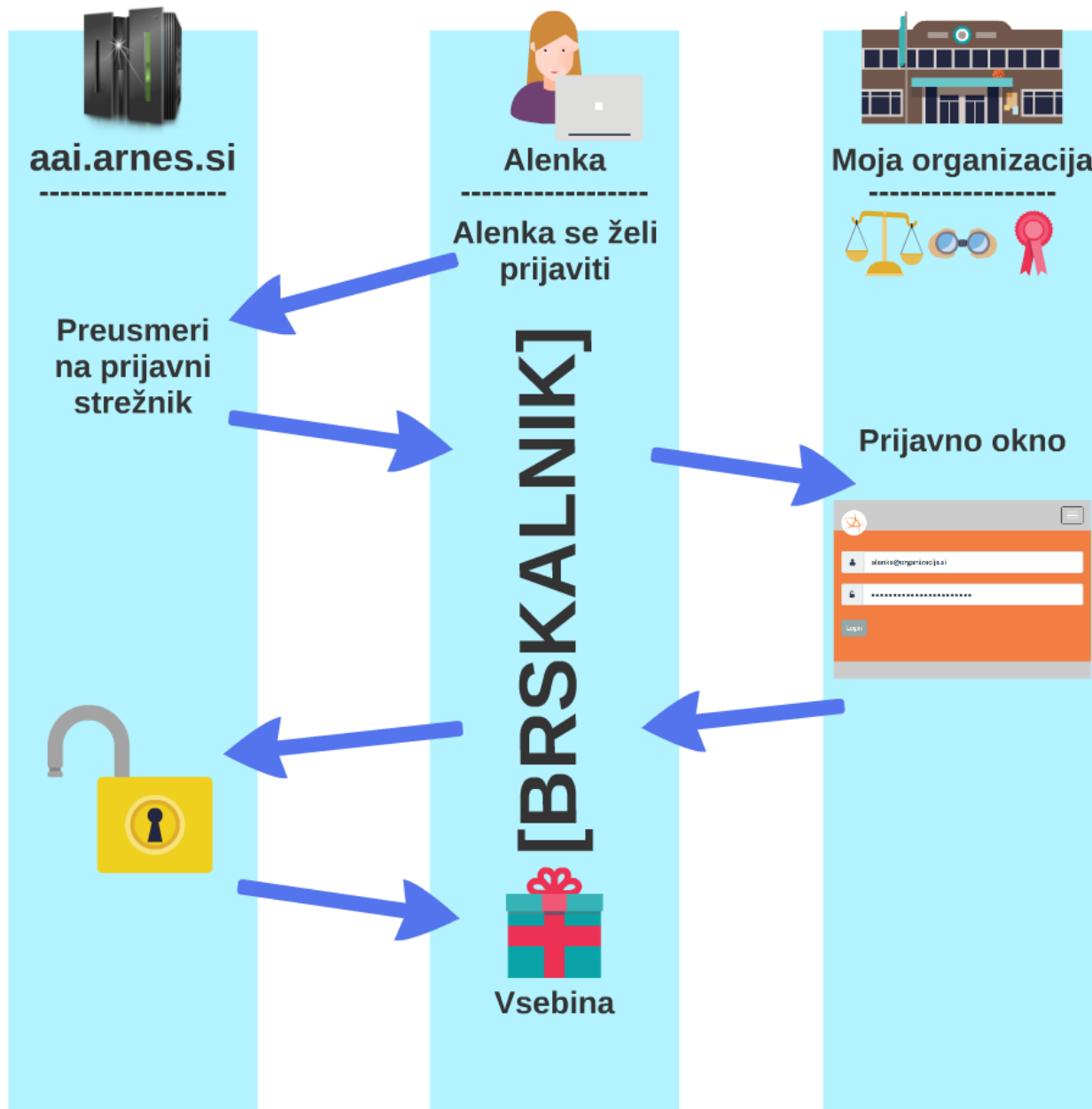
NetID

Ponudnik storitev

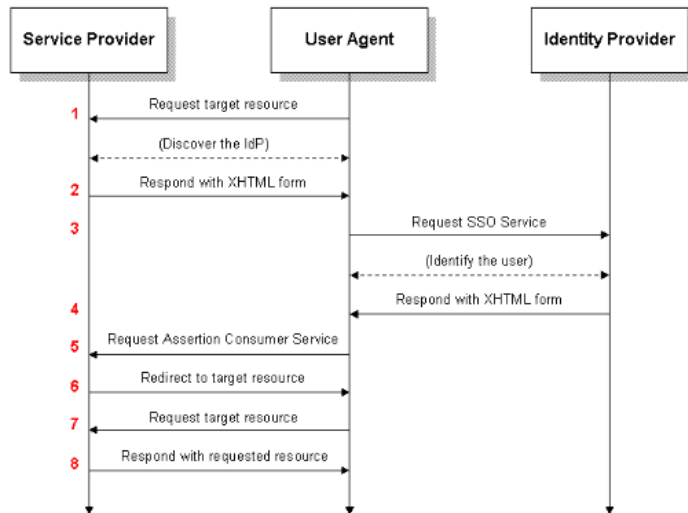
Simplesaml

Hudič je v podrobnostih!

Postopek enotne prijave (poenostavljeno)



Še bolj tehnično! ... s primeri



VIR: <https://en.wikipedia.org/wiki/File:Saml2-browser-ss0-post.gif>

Ponudnik storitev

- Polovica Shibboleth-a teče v spletnem strežniku (mod_shib_24.so)
- Na spletnem strežniku nastavimo pravila za dostop do virov
- Če uporabimo Shibboleth `<RequestMapper>` nastavimo tudi "ShibRequestSetting applicationId_ime_"
- Branje atributov (okoljske spremenljivke)

Okoljske spremenljivke enotne prijave:

Shib-Session-ID = `_cb9806872a3b3e0e544e1ff2de52dc67`

Shib-Identity-Provider = `https://centos.local/idp/20160122`

eduPersonPrincipalName = `up_ime@domena.si`

schacPersonalPosition = `urn:arnes.si:personalPosition:programer`

schacExpiryDate = ...

givenName = ...

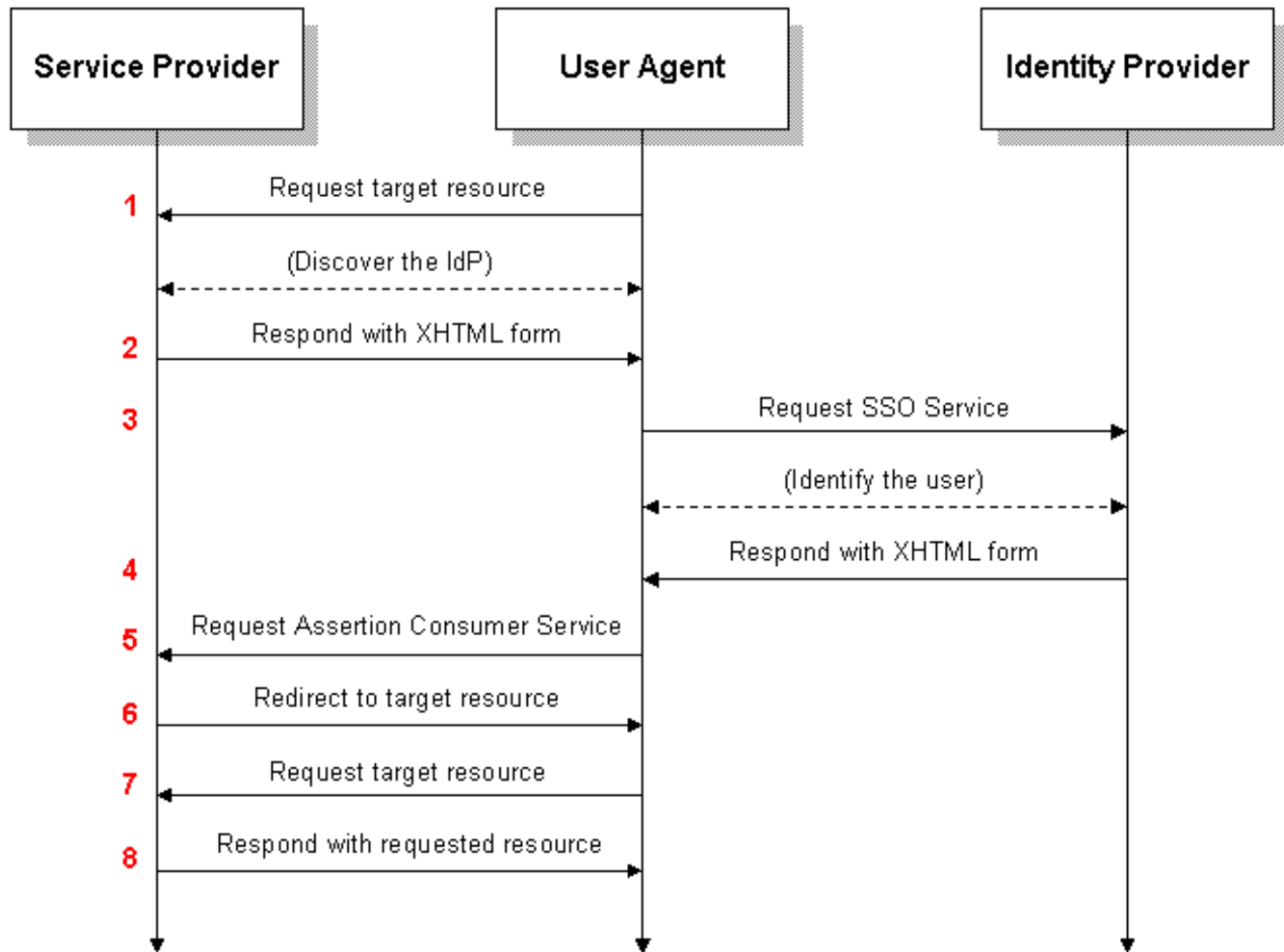
mail = ...

...

Branje v PHP:

```
$_SERVER["Shib-Identity-Provider"]
```

```
<Location /secure>
  AuthType Shibboleth
  ShibRequestSetting requireSession true
  Require Shibboleth
</Location>
```



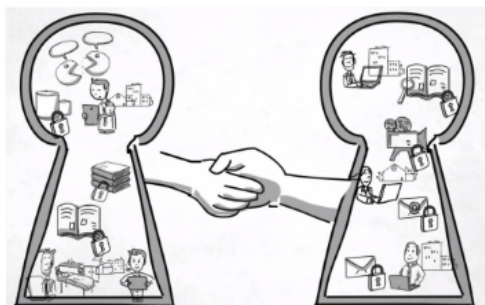
VIR: <https://en.wikipedia.org/wiki/File:Saml2-browser-sso-post.gif>

Kako pomembna je odjava?

- Nikoli ne puščamo odklenjenga avtomobila na javnem parkirišču (načeloma)
- Ne puščamo odklenjenih računalnikov
- Vedno poskrbimo za izpis z javnega računalnika!

Ali pač?

Tudi za odjavo je potrebno poskrbeti!



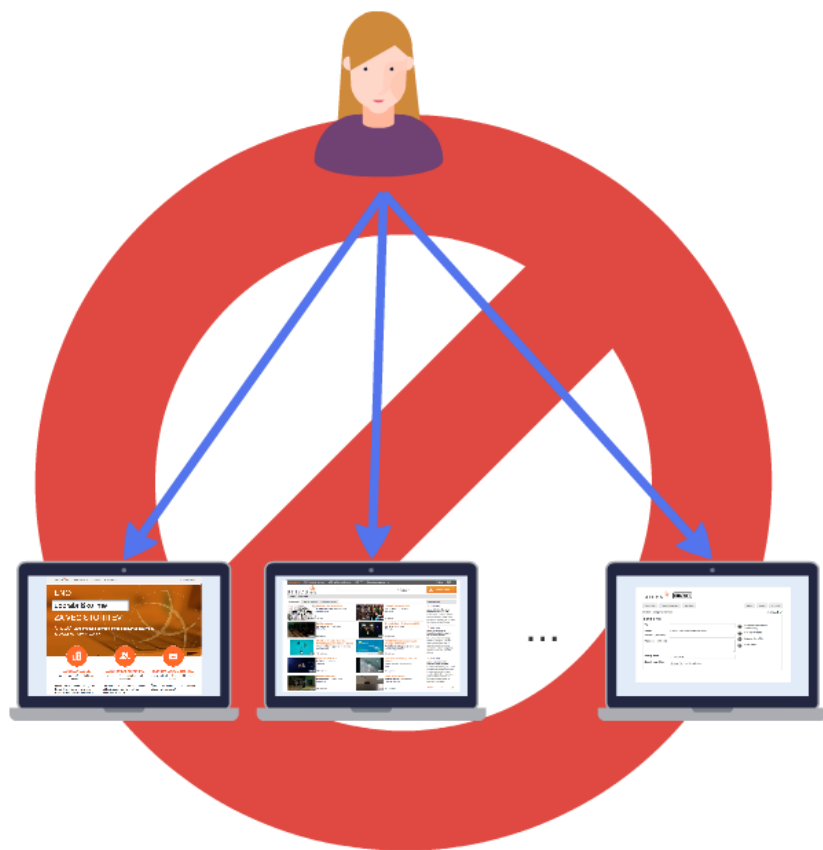
Damjana zanima ...



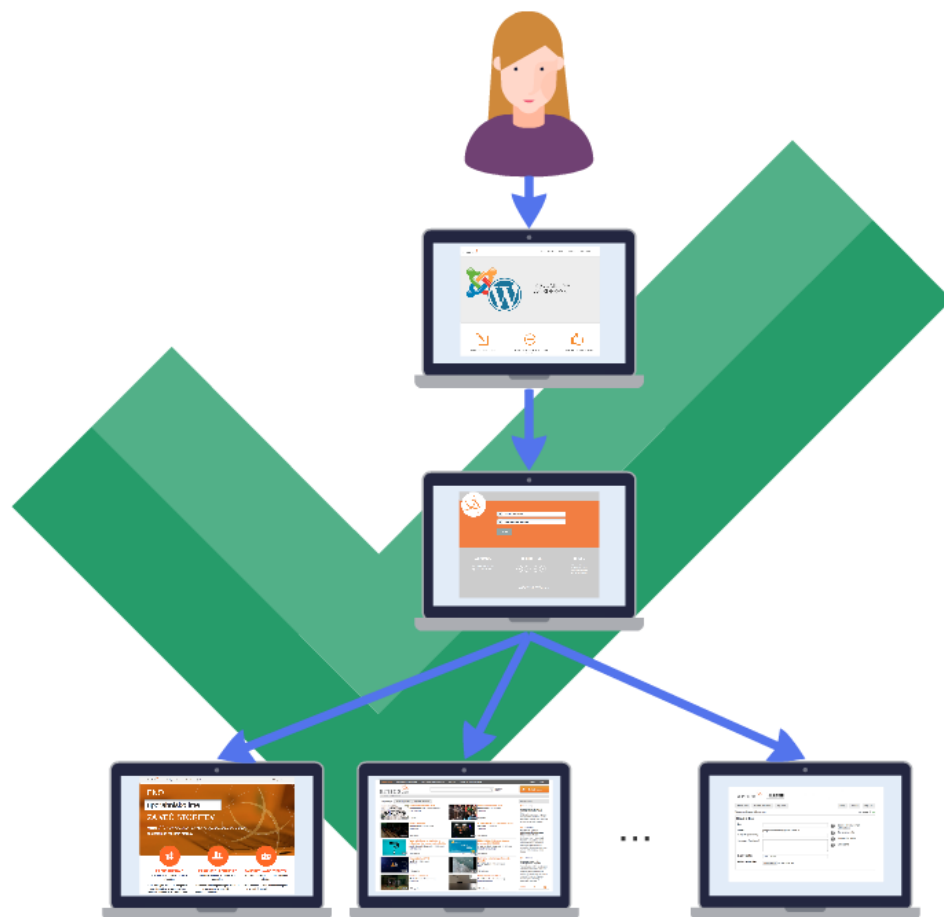
Kaj je SLO?

Single Log Out

Local Logout



Global Logout



<https://aai.arnes.si/aai/zarazvijalce>

Kaj to pomeni za skrbnike?

- Konfiguracija Shibboleth-a (prijavni vmesnik)
- Konfiguracija spletnega strežnika (Apache)
- Konfiguracija (ali popravek) aplikacije

<https://aai.arnes.si/aai/ponudnikstoritev>

Kapitan očitni pravi:

“Preden daš aplikacijo v produkcijo jo prej sam preizkusi, če ne deluje pa popravi!”

Session timeout

primer konfiguracije na: <https://aai.arnes.si/aai/ponudnikstoritev>

/etc/shibboleth/shibboleth2.xml :

```
<Sessions lifetime="28800" timeout="3600"  
  relayState="cookie" checkAddress="false"  
  handlerSSL="false" cookieProps="http"  
>
```

Potek uporabniške seje po 8 urah (oz. 28800 sekundah) in v primeru, da se uporabnik v roku ene ure ne uspe prijaviti tudi potče zahtevek.

Koliko časa naj bo seja aktivna je odvisno od uporabe/aplikacije

Aplikacijska seja

=/=

Shibboleth seja

Scope validation

Vsak (na novo) registriran ponudnik identitet ima parameter scope, ki določa katere realme (domena.si) lahko prijavlja.

Scope v metapodatkih:

```
<shibmd:Scope regexp="false">arnes.si</shibmd:Scope>
```

Vklop Scope validatorja na shibboleth-u:

attribute-map.xml:

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" id="eduPersonPrincipalName">  
  <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>  
</Attribute>  
<Attribute name="eduPersonPrincipalName" id="eduPersonPrincipalName">  
  <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>  
</Attribute>
```

attribute-policy.xml

```
<afp:AttributeRule attributeID="eduPersonPrincipalName">  
  <afp:PermitValueRuleReference ref="ScopingRules"/>  
</afp:AttributeRule>  
<afp:AttributeRule attributeID="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">  
  <afp:PermitValueRuleReference ref="ScopingRules"/>  
</afp:AttributeRule>
```



ARNES

aaa-podpora@arnes.si

januar 2016

Extra slide 1

Programski dostop do atributov

Primer prijave:

Osebni atributi:

- HTTP_EDUPERSONPRINCIPALNAME = profesor1@test-fed.arnes.si
- HTTP_DISPLAYNAME = Profesor
- HTTP_GIVENNAME = Profesor
- HTTP_CN = profesor1
- HTTP_SCHACHOMEORGANIZATION = test-fed.arnes.si
- HTTP_EDUPERSONPRIMARYAFFILIATION = faculty
- HTTP_SCHACDATEOFBIRTH = 19700101

Tehnični atributi:

- HTTP_SCHACEXPIRYDATE = 20371231235959Z
- HTTP_SCHACUUID = b28f20a0-74bb-452e-bb59-da3c99728e43
- HTTP_SHIB_SESSION_ID = _0234b7d98c584f1fe5f94ce63f6ad1b2
- HTTP_EDUPERSONTARGETEDID = 21d7503694562d66ad74a5837adc9b86ead6138b
- HTTP_SHIB_IDENTITY_PROVIDER = <https://idp.test-fed.arnes.si/idp/20081111>

Dostop do atributov v PHP-ju: `$_SERVER["HTTP_SHIB_IDENTITY_PROVIDER"]`

vir: <https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeAccess>

Extra slide 2

Enotna prijava & odjava

Ponudnik identitet

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="<https://idp.test-fed.arnes.si/simplesaml/saml2/idp/SingleLogoutService.php>"/>

<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="<https://idp.test-fed.arnes.si/simplesaml/saml2/idp/SSOService.php>"/>

Ponudnik Storitv:

<req:RequestInitiator Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-init"
Location="<https://centos/Shibboleth.sso/Login>"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="<https://sp.test-fed.arnes.si/Shibboleth.sso/SLO/SOAP>"/>

Extra slide 3

Več aplikacij na istem strežniku

shibboleth2.xml

```
...
<RequestMapper type="Native">
  <RequestMap applicationId="aplikacija1.primer.si">
    <Host name="aplikacija1.primer.si" applicationId="aplikacija1.primer.si" />
  </RequestMap>
  ...
</RequestMapper>
...
<ApplicationDefaults>
  ...
  <ApplicationOverride id="aplikacija1.primer.si" entityID="https://aplikacija1.primer.si/sp/20140707" REMOTE_USER="eppn
persistent-id targeted-id">
    <CredentialResolver type="File" key="aplikacija1.primer.si.key.pem" certificate="aplikacija1.primer.sicert.pem"/>
  </ApplicationOverride>
  ...
</ApplicationDefaults>
```

Apache vhost

```
<VirtualHost *:443>
  ServerName aplikacija1.primer.si
  ServerAdmin helpdesk@primer.si
  ...
  # Shibboleth settings
  <Location /prijava/aai/ >
    ShibRequestSetting applicationId aplikacija1.primer.si
    AuthType Shibboleth
    ShibRequireSession On
    require valid-user
    ShibRedirectToSSL 443
  </Location>
</VirtualHost>
```

Prenos parameterov

SP:

GET <https://sp.test-fed.arnes.si/secure>

302 <https://ds.test-fed.arnes.si/simplesaml/saml2/sp/idpdisco.php...>

DS:

GET <https://ds.test-fed.arnes.si/simplesaml/saml2/sp/idpdisco.php?entityID=https%3A%2F%2Fsp.test-fed.arnes.si>

302 <https://sp.test-fed.arnes.si/Shibboleth.sso/DS?SAMLDS=1&target=cookie%3Ab949e7bd&entityID=https%3A%2F%2Fidp.test-fed.arnes.si%2Fidp%2F20081111>

SP:

GET <https://sp.test-fed.arnes.si/Shibboleth.sso/DS?SAMLDS=1&target=cookie%3Ab949e7bd&entityID=https%3A%2F%2Fidp.test-fed.arnes.si>

302 <https://idp.test-fed.arnes.si/simplesaml/saml2/idp/SSOService.php?SAMLRequest=...>

IdP:

GET <https://idp.test-fed.arnes.si/simplesaml/saml2/idp/SSOService.php?SAMLRequest=...>

302 <https://idp.test-fed.arnes.si/simplesaml/module.php/core/loginuserpassorg.php?AuthState=...>

SP:

POST <https://sp.test-fed.arnes.si/Shibboleth.sso/SAML2/POST HTTP/1.1>

302 <https://sp.test-fed.arnes.si/secure>

SP:

GET <https://sp.test-fed.arnes.si/secure HTTP/1.1>

