

Instalace a konfigurace Shibboleth- Service Provider

Autor	Jaroslav Krotký, Milan Lysa, Jan Štikar
Verze dokumentu	v6
Datum	27.6.2024
Účel	Instalace a konfigurace Shibboleth - Service Provider

HISTORIE REVIZÍ				
Revize	Datum	Autor	Organizace	Popis
V4 (1.3)	01.01.2019	M. Lysa (KV)	Kraj Vysočina	Dopl. konfigurace Apache
v5 (1.4)	20.2.2019	D. Marek (KV)	Kraj Vysočina	Doplněna instalace a konfigurace v systému GNU/Linux.
v6	27.6.2024	J. Krotký (KV)	Kraj Vysočina	Změna na Authgate

1 Obsah

Obsah

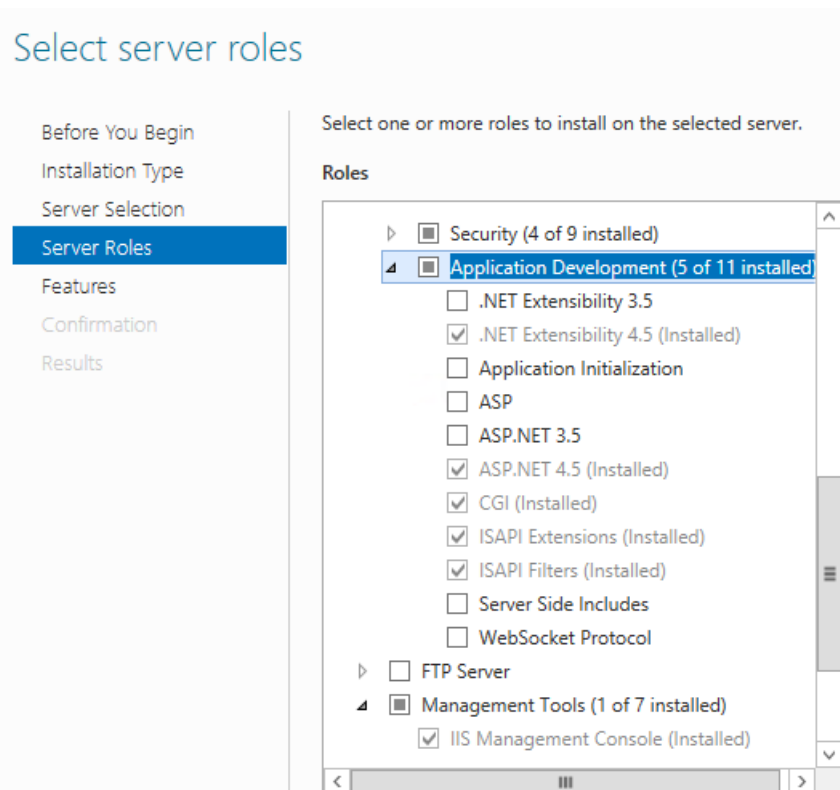
2	Popis	2
3	Windows	2
3.1	Instalace komponenty Shibboleth – SP	2
3.2	Konfigurace komponenty Shibboleth – SP pro webový server Microsoft IIS	5
3.3	Konfigurace komponenty Shibboleth – SP pro webový server Apache	7
	LoadModule mod_shib C:/Shibboleth/shibboleth-sp/lib64/shibboleth/mod_shib_24.so	7
4	Linux	8
4.1	Instalace Shibboleth SP pro Apache	8
4.2	Konfigurace Shibboleth SP pro Apache	8
4.2.1	Úprava konfiguračního souboru	8
4.2.2	Úprava šablony pro metadata	9
4.2.3	Vygenerování self-signed certifikátu	10
4.2.4	Vygenerování metadat a jejich registrace do IdP	10
4.3	Konfigurace web serveru Apache	10
4.3.1	Povolení modulu shibboleth v Apachi (a restart služby, aby se změny projeví):	10
4.3.2	Zakázání modulu shibboleth v Apachi (a restart služby, aby se změny projeví):	10
4.3.3	Úprava konfiguračního souboru Apache	10
5	Inicializace přihlášení uživatele a získání výsledku	11
	POZOR: naplnění hodnot serverových proměnných probíhá pouze do tzv. chráněných cest!	11
6	Užitečné odkazy	11
7	SHIBBOLETH2.XML - UKÁZKA	12

2 Popis

Tento dokument popisuje postup pro instalaci a konfiguraci komponenty Shibboleth Service Provider za účelem napojení webové aplikace do systému jednotného přihlašování federace Kraje Vysočina. Podrobně jsou zde rozepsány varianty instalace SP pro prostředí Windows a Linux s webovým serverem IIS a Apache. Oficiální instalační příručky najdete na stránce projektu Shibboleth: <https://wiki.shibboleth.net/confluence/display/SP3/Installation>.

3 Windows

V případě provozování Shibboleth SP na webovém serveru Microsoft IIS doporučujeme před instalací samotné komponenty nainstalovat nejdříve samotné IIS s nainstalovanými rolemi Application Development -> ISAPI Filters, CGI a pro konfiguraci IIS ještě roli Management tools -> IIS Management Console:



3.1 Instalace komponenty Shibboleth – SP

Komponenta vyžaduje nainstalované Visual C++ runtime libraries (dle verze 32 nebo 64 bit):

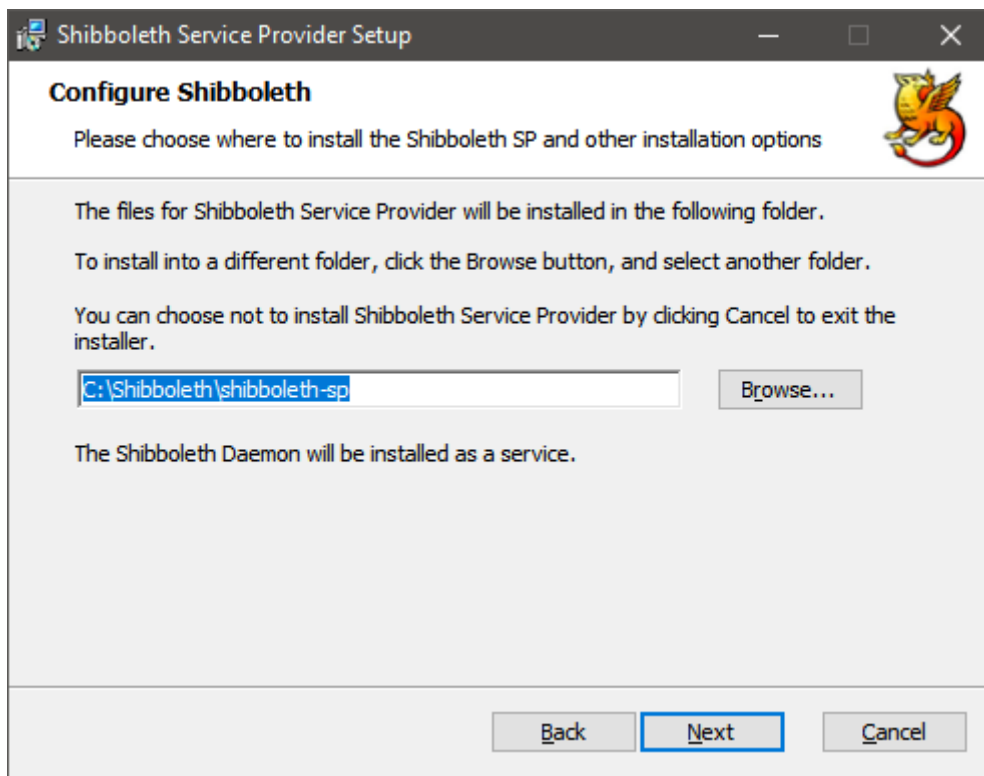
https://aka.ms/vs/15/release/VC_redist.x86.exe

https://aka.ms/vs/15/release/VC_redist.x64.exe

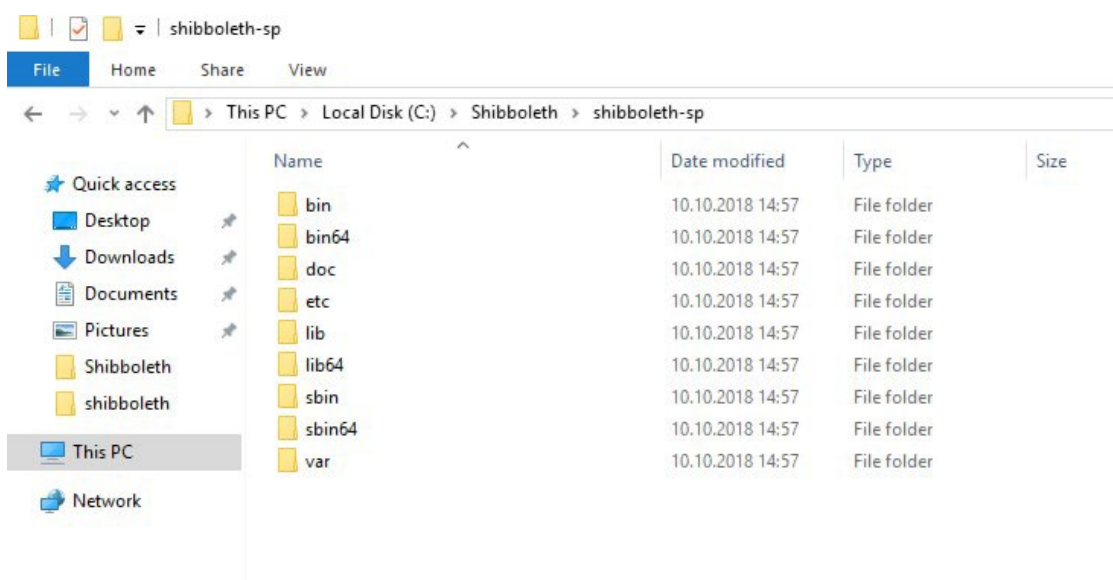
Aktuální verzi komponenty Shibboleth SP je možné stáhnout zde:

<https://shibboleth.net/downloads/service-provider/>

V průběhu instalace vyberte cestu, do které se komponenta nainstaluje:



Po instalaci by v daném adresáři měla vzniknout struktura:



Součástí instalace je i zaregistrování služby shibd_Default:

Name	PID	Description	Status	Group
SharedAccess		Internet Connection Sharing (ICS)	Stopped	netsvcs
ShellHWDetection	980	Shell Hardware Detection	Running	netsvcs
shibd_Default	3276	Shibboleth Daemon (Default)	Running	

V IIS Management konzoli zkontrolujte, zda se provedla i registrace Shibboleth SP do IIS – mapování requestů *.sso na ISAPI modul (isapi_shib.dll):

Name	Path	State	Path Type	Handler	Entry Type
ScriptHandlerFactoryAppServ...	*_AppService.axd	Enabled	Unspecified	System.Web.Script.Services.S...	Local
ScriptResourceIntegrated-4.0	*ScriptResource.axd	Enabled	Unspecified	System.Web.Handlers.ScriptR...	Local
Shibb	*.sso	Enabled	File	IsapiModule	Local
SimpleHandlerFactory-Integra...	*.ashx	Enabled	Unspecified	System.Web.UI.SimpleHandle...	Local
SimpleHandlerFactory-ISAPI-4...	*.ashx	Enabled	Unspecified	IsapiModule	Local

Dále zkontrolujte, zda je povoleno volání samotné CGI extension Shibboleth SP:

Description	Restriction	Path
[No Description]	Allowed	C:\Shibboleth\shibboleth-sp\lib64\shibboleth\isapi_shib.dll
ASP.NET v4.0.3...	Allowed	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
ASP.NET v4.0.3...	Allowed	%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll

A Zkontrolovat registrované Moduly (Native) v rootu serveru, ne na Web site, tam chybí tlačítko proregistraci), zda jsou registrované „Native“ moduly ShibNative a ShibNative32:

Name	Code	Module Type	Entry Type
AnonymousAuthenticationM...	%windir%\System32\inetrv\authanon.dll	Native	Local
AnonymousIdentification	System.Web.Security.AnonymousIdentificationModule	Managed	Local
Session	System.Web.SessionState.SessionStateModule	Managed	Local
ShibNative	C:\shibboleth-sp\lib64\shibboleth\iis7_shib.dll	Native	Local
ShibNative32	C:\shibboleth-sp\lib\shibboleth\iis7_shib.dll	Native	Local

Pokud konfigurace IIS neproběhla, je třeba přidat výše uvedené ručně:

1. V ISAPI Filters: Add... Filter name: Shibboleth, Executable: C:\Shibboleth\shibboleth-sp\lib64\shibboleth\isapi_shib.dll
2. V Handler Mappings: Add Script Map... Request path: *.sso, Executable:

- C:\Shibboleth\shibboleth-sp\lib64\shibboleth\isapi_shib.dll, Name: Shibboleth, V Request Restrictions: záložka Mapping odebrat „Invoker handler only if ...“
3. Krok 2 by měl při uložení nabídnout přidání DLL souboru do ISAPI and CGI Restrictions, následně by se měl v záložce „ISAPI and CGI Restrictions“ objevit řádek pro Shibboleth SP.
 4. Zaregistrovat v Modules tyto Native moduly:
 - ShibNative = C:\Shibboleth\shibboleth-sp\lib64\shibboleth\iis7_shib.dll
 - ShibNative32 = C:\Shibboleth\shibboleth-sp\lib\shibboleth\iis7_shib.dll
 5. Restartovat IIS

Pokud instalace proběhla správně a je spuštěna služba shibd_Default, tak by po zadání adresy <http://localhost/Shibboleth.sso/Status> měl být vidět stav komponenty.

3.2 Konfigurace komponenty Shibboleth – SP pro webový server Microsoft IIS

Jako první je potřeba upravit soubor C:\Shibboleth\shibbolethsp\etc\shibboleth\shibboleth2.xml, podstatné je však správně nastavit následující hodnoty elementů:

- **InProcess -> ISAPI -> Site:** v atributu „id“ je třeba vyplnit id stránky dle IIS, v atributu „name“ nastavit URL aplikace, scheme=“https“ a nastavit číslo portu (výchozí 443).
- **RequestMapper -> RequestMap -> Host:** hodnota atributu „name“ musí odpovídat hodnotě „name“ v elementu Site. V elementech Path jsou uvedené cesty URL, které budou automaticky zabezpečené autentizací Shibboleth a zároveň pro ně budou naplněny hodnoty serverových proměnných o přihlášeném uživateli.
- **ApplicationDefaults:** v atributu „entityID“ nastavte unikátní identifikátor poskytovatele
- služby, pod kterým bude SP dále vystupovat a neměl by být měněn. Tvar identifikátoru je https://vaše_doména/shibboleth
- **Sessions:** pokud bylo v elementu Site zvolené schéma HTTPS, nastavte i odpovídající hodnoty atributů: handlerSSL="true" a cookieProps="https" a nastavte následující handlers:
 - Handler type="MetadataGenerator" a template="metadata-template.xml"
 - Handler type="Status": nastavte oprávnění v atributu „acl“ kde uveďte mezerou oddělené adresy, z kterých má být přístupný stav komponenty.
- **Errors:** vyplnit kontakt, který se zobrazí uživateli v případě neočekávané chyby.
- **MetadataProvider:** nastavte způsob, kde bude Shibboleth SP načítat informace o identity providerech. Typicky to bude buď lokální soubor, který budeme muset ručně upravovat a udržovat aktuální nebo využijete veřejně publikovaná metadata:
 - atribut path="partner-metadata.xml" pro lokální soubor.
 - Atribut url="https://ds-ts.kr-vysocina.cz:8443/metadata/vysocinaid+idp.xml" s uvedením adresy, nastavení záložního souboru v atributu „backingFilePath“ a max. doby platnosti lokálních údajů „maxRefreshDelay“.
- **AttributeExtractor:** odkaz na konfiguraci mapování atributů převzatých od IdP ze SAMLAssertion - path="attribute-map.xml".
- **AttributeFilter:** odkaz na konfiguraci filtrování atributů od IdP - path="attribute-policy.xml".
- **Sessions:** <!-- single IdP --> <SSO entityID="https://authgate-ts.kr-vysocina.cz/authgateService">SAML2</SSO> viz kap. 7 SHIBBOLETH2.XML

Dále je potřeba upravit šablonu pro generování metadat v souboru
C:\Shibboleth\shibbolethsp\etc\shibboleth\metadata-template.xml:

EntityDescriptor -> SPSSODescriptor a nastravit hodnoty následujících elementů:

- mdui:**UIInfo**: názvy, popisy, informace a odkaz na logo service providera
- md:**Organization**: informace o organizaci provozující aplikaci
- md:**ContactPerson**: kontaktní osoba / správce service providera

Dále je třeba upravit mapování atributů předaných od IdP do serverových proměnných v souboru

C:\Shibboleth\shibbolethsp\etc\shibboleth\attribute-map.xml

uid	eppn, REMOTE_USER
mail	e-mail uživatele
postOfficeBox	IČO příspěvkové organizace Kraje Vysočina

Doplnit:

```
<Attribute name="urn:oid:0.9.2342.19200300.100.1.1" id="uid"/>
```

```
<Attribute name="urn:mace:dir:attribute-def:uid" id="uid"/>
```

```
<Attribute name="urn:oid:0.9.2342.19200300.100.1.3" id="mail"/>
```

```
<Attribute name="urn:mace:dir:attribute-def:mail" id="mail"/>
```

```
<Attribute name="urn:oid:2.5.4.18" id="postOfficeBox"/>
```

```
<Attribute name="urn:mace:dir:attribute-def:postOfficeBox" id="postOfficeBox"/>
```

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" id="eduPersonAffiliation"/>
```

```
<Attribute name="urn:mace:dir:attribute-def:eduPersonAffiliation" id  
="eduPersonAffiliation"/>
```

```
<Attribute name="urn:oid:2.5.4.42" id="givenName"/>
```

```
<Attribute name="urn:mace:dir:attribute-def:givenName" id="givenName"/>
```

```
<Attribute name="urn:oid:2.5.4.3" id="cn"/>
```

```
<Attribute name="urn:mace:dir:attribute-def:cn" id="cn"/>
```

```
<Attribute name="urn:oid:2.5.4.4" id="sn"/>
```

```
<Attribute name="urn:mace:dir:attribute-def:sn" id="sn"/>
```

Po vyplnění a restartu služby jsou dostupné vygenerované metadata pro SP na stránce

<http://localhost/Shibboleth.sso/Metadata>

Tyto metadata je pak třeba doplnit u konkrétních Identity Providerů případně je přidat do federálních metadat a je třeba je udržovat konzistentní u každého SP, IdP a DS. Konkrétně pro SP se to týká udržování aktuálního souboru „partner-metadata.xml“ nebo využití veřejných metadat publikovaných na webové URL <https://ds-ts.kr-vysocina.cz:8443/metadata/vysocinaid+idp.xml>.

3.3 Konfigurace komponenty Shibboleth – SP pro webový server Apache

Jako první je potřeba upravit soubor C:\Shibboleth\shibbolethsp\etc\shibboleth\shibboleth2.xml.

Pro Apache server je možné smazat elementy **InProcess** a **RequestMapper**.

- **ApplicationDefaults:** v atributu „entityID“ nastavte unikátní identifikátor poskytovatele
- služby, pod kterým bude SP dále vystupovat a neměl by být měněn. Tvar identifikátoru je `https://vaše_doména/shibboleth`
- **Sessions:** pokud bylo v elementu Site zvolené schéma HTTPS, nastavte i odpovídající hodnoty atributů: `handlerSSL="true"` a `cookieProps="https"` a nastavte následující handlers:
 - `Handler type="MetadataGenerator"` a `template="metadata-template.xml"`
 - `Handler type="Status"`: nastavte oprávnění v atributu „acl“ kde uveďte mezerou oddělené adresy, z kterých má být přístupný stav komponenty.
- **Errors:** vyplnit kontakt, který se zobrazí uživateli v případě neočekávané chyby.
- **MetadataProvider:** nastavte způsob, kde bude Shibboleth SP načítat informace o identity providerech. Typicky to bude buď lokální soubor, který budeme muset ručně upravovat a udržovat aktuální nebo využijete veřejně publikovaná metadata:
 - atribut `path="partner-metadata.xml"` pro lokální soubor.
 - Atribut `url="https://ds-ts.kr-vysocina.cz:8443/metadata/vysocinaid+idp.xml"` s uvedením adresy, nastavení záložního souboru v atributu „backingFilePath“ a max. doby platnosti lokálních údajů „maxRefreshDelay“.
- **AttributeExtractor:** odkaz na konfiguraci mapování atributů převzatých od IdP ze SAMLAssertion - `path="attribute-map.xml"`.
- **AttributeFilter:** odkaz na konfiguraci filtrování atributů od IdP - `path="attribute-policy.xml"`.
- **Sessions:** `<!-- single IdP --> <SSO entityID="https://authgate-ts.kr-vysocina.cz/authgateService">SAML2</SSO>` viz kap. 7 SHIBBOLETH2.XML

Dále v souboru Apache/conf/httpd.conf provedete aktivování modulu Shibboleth SP, vyberte modul SO z adresáře odpovídajícímu sestavení Apache (pro 32bit je to lib32, pro 64-bit pak lib64):

LoadModule mod_shib C:/Shibboleth/shibboleth-sp/lib64/shibboleth/mod_shib_24.so

ShibCompatValidUser On/Off nastavíme na On, pokud chceme chránit určitou cestu automaticky na základě pravidel „require valid-user“ nebo na Off, pokud budeme přihlášení uživatele řídit na aplikační úrovni.

Pro server nebo pro vybraného vhosta doplníme následující konfigurační hodnoty:

```
<Location /Shibboleth.sso>
  AuthType None
  Require all granted
</Location>

<IfModule mod_alias.c>
  <Location /shibboleth>
    AuthType None
    Require all granted
  </Location>
```

```
Alias /shibboleth/main.css C:/Shibboleth/shibboleth-sp/doc/shibboleth/main.css
</IfModule>
```

Případně uvést i chráněné cesty:

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

Po restartu Apache by mělo být dostupné zjištění stavu komponenty Shibboleth SP:

<http://localhost/Shibboleth.sso/Status>

a mělo by být funkční i stažení metadat:

<http://localhost/Shibboleth.sso/Metadata>

4 Linux

Instalace a konfigurace Shibboleth SP je popsána pro distribuci Debian a webový server Apache. Instalace a konfigurace na jiných distribucích se může mírně lišit. Příkazy psané kurzívou je nutné spouštět s potřebnými oprávněními.

4.1 Instalace Shibboleth SP pro Apache

Nejprve je potřeba nainstalovat balík libapache2-mod-shib2. Tento balík obsahuje jak shibboleth module pro webový server Apache, tak podpůrného daemona:

```
- apt install libapache2-mod-shib2
```

Při instalaci je nutné přijmout instalaci všech závislostí. Samotná instalace automaticky povolí modul v Apachi.

Příkazy

4.2 Konfigurace Shibboleth SP pro Apache

4.2.1 Úprava konfiguračního souboru

Konfigurační soubor je /etc/shibboleth/shibboleth.xml. V tomto XML souboru je potřeba editovat níže uvedené elementy uvedeným způsobem. Tučně zvýrazněné hodnoty atributů je potřeba přizpůsobit konkrétní aplikaci:

4.2.1.1 *Element RequestMapper*

```
<RequestMapper type="Native">
  <RequestMap applicationId="default">
    <Host name="https://URL aplikace">
      <Path name="secure" authType="shibboleth" requireSession="true"/>
    </Host>
  </RequestMap>
</RequestMapper>
```

4.2.1.2 *Element ApplicationDefaults*

```
<ApplicationDefaults entityID="https://URL aplikace/shibboleth"
    REMOTE_USER="eppn persistent-id targeted-id"
    cipherSuites="ECDHE+AESGCM:ECDHE:!aNULL:!eNULL:!LOW:!EXPORT:!RC4:!SHA:!SSLv2">
```

4.2.1.3 *Element SSO*

```
<SSO discoveryProtocol="SAMLDS" discoveryURL="https://ds.kr-vysocina.cz/discovery/DS">
    SAML2 SAML1
</SSO>
```

4.2.1.4 *Element Handler MetadataGenerator*

```
<Handler type="MetadataGenerator" Location="/Metadata" signing="false"
template="/etc/shibboleth/cesta_k_sablone/sablona.xml"/>
</Sessions>
```

4.2.1.5 *Element Errors*

```
<Errors supportContact="shibboleth@kr-vysocina.cz"
    helpLocation="/about.html"
    styleSheet="/shibboleth-sp/main.css"/>
```

4.2.1.6 *Element MetadataProvider*

```
<MetadataProvider type="XML" validate="true" uri="https://ds.kr-
vysocina.cz/metadata/vysocinaid+idp.xml" file="partner-metadata.xml"/>
```

4.2.2 *Úprava šablony pro metadata*

Šablona musí být umístěna tam, kde bylo specifikováno v elementu Handler typu MetadataGenerator. Defaultní umístění bývá /etc/shibboleth/sablona.xml. Obsah šablony by měl být následující (tučně zvýrazněné hodnoty je potřeba upravit dle aplikace):

```
<?xml version="1.0" encoding="utf-8" ?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:SPSSODescriptor>
    <!-- pridani endpointu pro alternativni DNS jmena -->
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://URL aplikace/Shibboleth.sso/SAML2/POST" index="1"/>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://URL aplikace/Shibboleth.sso/SAML2/POST" index="2"/>
  </md:SPSSODescriptor>
  <md:Organization>
    <md:OrganizationName xml:lang="en">Kraj Vysocina</md:OrganizationName>
    <md:OrganizationName xml:lang="cs">Kraj Vysocina</md:OrganizationName>
    <md:OrganizationDisplayName xml:lang="en">Kraj Vysocina</md:OrganizationDisplayName>
    <md:OrganizationDisplayName xml:lang="cs">Kraj Vysocina</md:OrganizationDisplayName>
    <md:OrganizationURL xml:lang="en">https://www.kr-vysocina.cz/en</md:OrganizationURL>
    <md:OrganizationURL xml:lang="cs">https://www.kr-vysocina.cz/</md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="technical">
    <md:GivenName>Jméno</md:GivenName>
    <md:SurName>Příjmení</md:SurName>
    <md:EmailAddress>shibboleth@kr-vysocina.cz</md:EmailAddress>
```

```
</md:ContactPerson>  
</md:EntityDescriptor>
```

4.2.3 Vygenerování self-signed certifikátu

Pro účely šifrování a podepisování je potřeba vygenerovat self-signed certifikát:

```
shib-keygen -h sluzba.organizace.cz -y 10 -e https://sluzba.organizace.cz/shibboleth
```

kde parametry:

- h je hostname serveru, kde služba běží
- y 10 je platnost certifikátu v rocích
- e je entityID, pro které certifikát vystavujeme

4.2.4 Vygenerování metadat a jejich registrace do IdP

Po úpravách konfigurace Shibboleth SP je potřeba službu restartovat:

- *service shibd restart*

a vygenerovat metada na URL:

- *https://URL aplikace/Shibboleth.sso/Metadata*

a nechat je zaregistrovat do IdP.

4.3 Konfigurace web serveru Apache

4.3.1 Povolení modulu shibboleth v Apachi (a restart služby, aby se změny projevily):

- *a2enmod shib2*
- *service apache2 restart*

4.3.2 Zakázání modulu shibboleth v Apachi (a restart služby, aby se změny projevily):

- *a2dismod shib2*
- *service apache2 restart*

4.3.3 Úprava konfiguračního souboru Apache

Umístění konfiguračního souboru Apache se může lišit v závislosti na způsobu jeho implementace a distribuci. Př. umístění může být /etc/apache2/sites-available/aplikace.conf (nebo /etc/apache2/apache2.conf).

Do souboru je potřeba přidat tuto autentizační konfiguraci do directory s aplikací, která se týká autentizace:

```
AllowOverride None  
Allow from all  
AuthType shibboleth  
ShibDisable Off  
ShibRequireSession On  
ShibUseHeaders On  
require shibboleth  
require valid-user
```

Dále přidat modul:

```
<Location /Shibboleth.sso>
    SetHandler shib
    Require all granted
    Order allow,deny
    Allow from all
    Deny from none
</Location>
```

A dále:

```
<IfModule mod_alias.c>
<Location /shibboleth-sp>
    Allow from all
</Location>
Alias /shibboleth-sp/main.css /usr/local/share/doc/shibboleth/main.css
Alias /shibboleth-sp/logo.jpg /usr/local/share/doc/shibboleth/logo.jpg
</IfModule>
```

Aby se změny promítly:

- *service apache2 restart*

5 Inicializace přihlášení uživatele a získání výsledku

Přihlášení uživatele proběhne buď automaticky při přístupu na některou ze zabezpečených cest uvedených v konfiguraci „shibboleth2.xml“ v elementu RequestMapper -> RequestMap -> Host.

Druhou možností je přesměrovat uživatele na adresu [https://domena\(:port\)/Shibboleth.sso/Login](https://domena(:port)/Shibboleth.sso/Login) s možností uvést v parametru „target“ návratovou URL (URL encoded), na kterou bude po přihlášení uživatelův browser přesměrován: [https://domena\(:port\)/Shibboleth.sso/Login?target=URL_adresa](https://domena(:port)/Shibboleth.sso/Login?target=URL_adresa).

Výsledek přihlášení uživatele uloží komponenta do tzv. server variables. Přístup k nim je specifický pro jednotlivé jazyky:

<https://wiki.shibboleth.net/confluence/display/SP3/AttributeAccess>

Unikátní jméno autentizovaného uživatele je dostupné v proměnné REMOTE_USER.

POZOR: naplnění hodnot serverových proměnných probíhá pouze do tzv. chráněných cest!

Stav session uživatele je možné ověřit na adrese <https://SERVERNAME/Shibboleth.sso/Session>

6 Užitečné odkazy

Shibboleth service provider:

<https://wiki.shibboleth.net/confluence/display/SP3>

Instalace Shibboleth SP pro Linux:

<https://wiki.shibboleth.net/confluence/display/SP3/LinuxInstall>

Instalace Shibboleth SP pro Windows:

<https://wiki.shibboleth.net/confluence/display/SP3/Install+on+Windows>

Shibboleth eduID.cz

<https://www.eduid.cz/cs/tech/sp/shibboleth>

Stažení klienta SP:

<https://shibboleth.net/downloads/service-provider/>

7 SHIBBOLETH2.XML - UKÁZKA

<https://extranet.kr->

[vysocina.cz/shibboleth/shibboleth2.zip](https://extranet.kr-vysocina.cz/shibboleth/shibboleth2.zip)