1 OpenID klient

Tento dokument popisuje ukázku základní implementace klienta, který umožňuje praktické využití standardu OpenID pro jednotné přihlašování uživatelů do systému poskytovatelů (firem). V tomto případě ukazuje, jak prakticky realizovat přihlášení uživatele a získání dat uživatele pomocí služby MojeID. MojeID je implementace standardu OpenID od sdružení CZ.NIC. Standard obecně je platformě nezávislý, pro komunikaci využívá protokol HTTP resp. jeho zabezpečenou verzi HTTPS. Celá komunikace probíhá pomocí přesměrování uživatelova prohlížeče z webu poskytovatele služby na OpenID klienta, potom dále na službu MojeID a zpět na OpenID klienta a na web poskytovatele. Ukázkový klient je vytvořen pro platformu Java.

1.1 Slovník pojmů:

realm – určuje oblast URL, ze které budou chodit požadavky na MojeID server. Všechny požadavky i návratová adresa (viz. returnUrl) musejí ležet v tomto realm. Realm je nutné dohodnout s CZ.NIC.
returnUrl – návratová adresa, kam bude uživatel přesměrován po provedení autentizace pomocí MojeID
endpoint – adresa serveru MojeID, existuje testovací a produkční prostředí

Před zahájením implementace je vhodné přečíst oficiální dokumentaci k MojeID od CZ.NIC (www.mojeid.cz), kde je dostatečně popsán celý proces, jak MojeID pracuje a komunikuje s poskytovatelem služeb. Vhodné je začít dokumentem „01-mojeid__technicky_popis.pdf", který je přiložen i k tomuto dokumentu ve složce /docs.

1.2 Stručný popis klienta:

Jde o servlet, který poslouchá na určité URL a zabezpečuje tyto činnosti:

- přijímá požadavky na přihlášení pomocí MojeID od serveru poskytovatele
- iniciuje spojení s MojeID serverem
- přesměruje uživatele na web MojeID, kde dojde k autentizaci uživatele
- přijímá odpověď ze serveru MojeID
- provádí ověření pravosti odpovědi ze serveru MojeID (ověření platnosti autentizace uživatele na serveru MojeID)
- získání ověřeného identifikátoru uživatele a dalších jeho osobních údajů, předávaných poskytovateli služby
- vyhodnocuje zprávy o chybném přihlášení
- rozhoduje o přesměrování uživatele po úspěšném provedení autentizace

1.3 Postup zpracování

Detailní postup, jak probíhá komunikace mezi mojeID serverem a klientem, je popsána v dokumentaci MojeID, konkrétně v dokumentu „01-mojeid__technicky_popis.pdf", který naleznete ve složce /docs.

1.4 Postup nasazení OpenID klienta:

- volba webového serveru, na kterém bude nasazen OpenID klient. Server by měl pracovat s protokolem HTTPS, tedy podporovat zabezpečené spojení. Pro testovací provoz toto ale není podmínkou. Lze použít například Apache Tomcat.
- Definovat hodnotu realm a dohodnout se na jejím použití s CZ.NIC. V realm musí ležet URL, na které poslouchá servlet OpenID klienta. Lze použít např. URL webového serveru.
- Nastavení hodnoty realm.
  Vaši hodnotu realm lze nastavit do proměnné REALM ve třídě ConsumerServlet.
- Nastavení hodnoty DEFAULT_MOJEID_ENDPOINT ve třídě ConsumerServlet.
  Hodnotu lze ponechat na https://mojeid.cz/endpoint/, jde o produkční MojeID server.
- Nastavení v xrds.xml v projektu ve složce WEB-INF.
  Do tagu URI je nutné zapsat návratovou URL adresu, kam má být uživatel přesměrován po provedení autentizace na MojeID serveru. V tomto případě jde o URL OpenID klienta včetně parametru is_return, který informuje o tom, že jde o odpověď z mojeID serveru, kterou má klient zpracovat.
  <URI>https://vasserver.cz/OpenIdClientSample/consumer?is_return=true</URI>
- Sestavení a nasazení projektu OpenIdClientSample na server.
- Vstup na úvodní stránku https://vasserver.cz/OpenIdClientSample/index.jsp.

1.5 Informace k ukázkovém klientovi:

- klient je vytvořen jako projekt v IDE Eclipse a naleznete ho ve složce /projekt
- výchozí stránkou aplikace je ../OpenIdClientSample/index.jsp, tato stránka simuluje výchozí web, kde uživatel začíná, může jít například o web firmy. Stránka obsahuje pouze tlačítko "Přihlásit pomocí MojeID". Index.jsp je zároveň návratovou stránkou, kam je uživatel přesměrován po úspěšné autentizaci. Stránka v tomto případě zobrazí seznam předaných osobních údajů z MojeID.
- Servlet realizující přihlášení poslouchá na URL ../OpenIdClientSample/consumer. Na tuto URL přesměrovává i tlačítko "Přihlásit pomocí MojeID" na stránce index.jsp. Servlet očekává v parametru frontendUrl adresu, na kterou bude uživatel OpenID klientem přesměrován po úspěšné autentizaci a zpracování OpenID klientem.
- Pro komunikaci se serverem MojeID je použita open source knihovna OpenId4Java. Náš klient používá pouze část funkcionality této knihovny, která toho nabízí mnohem více. Oficiální dokumentaci naleznete na adrese: http://code.google.com/p/openid4java/.
  Klient využívá pouze mechanismus iniciace spojení, vytvoření žádosti o

autentizaci, ověření platnosti odpovědi od serveru MojeID a nakonec získání osobních údajů uživatele.
- Důležité jsou parametry realm a returnUrl. Jejich význam je popsán výše.
- Všechny potřebné knihovny jsou uloženy v adresáři /projekt/lib v projektu. Důležitá je knihovna openid4java-0.9.6.jar.
- xrds.xml – jde o XML **dokument, vystavený na URL odpovídající realm**. V dokumentu je uvedena hodnota návratové URL adresy, která se musí shodovat s návratovou adresou (parametr returnToUrl), předanou OpenID klientem při vytváření autorizačního požadavku (viz metoda ConsumerServlet.authOpenIdRequest).
  Dokument obsahuje tag Service s tagy Type a URI. Ukázka jeho obsahu:

```
<?xml version="1.0" encoding="UTF-8"?>
<xrds:XRDS xmlns:xrds="xri://$xrds" xmlns="xri://$xrd*($v*2.0)">
    <XRD>
            <Service>
                    <Type>http://specs.openid.net/auth/2.0/return_to</Type>
                    <URI>https://vasserver.cz/OpenIdClientSample/consumer?is_return=true</URI>
            </Service>
    </XRD>
</xrds:XRDS>
```

  Do tagu URI je nutné zapsat návratovou URL adresu, kam má být uživatel přesměrován po provedení autentizace na MojeID serveru. V tomto případě jde o URL OpenID klienta včetně parametru is_return, který informuje o tom, že jde o odpověď z MojeID serveru, kterou má klient zpracovat.
  Poté co je uživatel přesměrován na MojeID server a provede přihlášení, pokusí se MojeID server ověřit návratovou URL adresu, která mu byla předána během vytváření autentizačního požadavku. Hodnota se musí rovnat údaji uvedenému v xrds.xml v tagu URI.
- Ostatní detaily jsou popsány v Javadoc komentářích přímo v kódu.

1.6 Tipy v případě problémů:

- Zkontrolovat nastavení firewallů, zda neblokují komunikaci mezi vaším webovým serverem a MojeID serverem.
- Dohodnout se na používání realm s CZ.NIC.
- Zkontrolovat správnou hodnotu URI v xrds.xml.

1.7 Příloha

Obsah zip souboru obsahuje tyto adresáře:
/projekt - projekt OpenIdClientSample v IDE Eclipse
/docs - přiložené dokumenty

1.8 Kontakty

V případě dotazů se obracejte na: info@active24.cz