MojeID

Technické podmínky provozu

Obsah

1 Úvod

Tento dokument obsahuje obecný úvod do principů a fungování služby mojeID. Naleznete zde také ukázkové scénáře, příklady a další obecné informace, které Vám pomohou navrhnout jakým způsobem implementovat podporu služby mojeID do Vaší webové aplikace. Získáte tak rychlý základní přehled o krocích, které bude potřeba provést při implementaci podpory mojeID a budete moci odhadnout náročnost této implementace.

Návody, detaily a zdrojové kódy pro konkrétní programovací jazyky jsou k dispozici v přiložených dokumentech. Naleznete v nich krok po kroku vysvětlený postup jak začít s existujícím/novým projektem a zabudovat do něj podporu pro mojeID. Pro čtení těchto dokumentů se doporučuje znalost tohoto textu.

2 Terminologie

V dalších kapitolách týkajících se implementace mojeID bude používána následující terminologie:

•**Identifikátor** – URL se schématem „http“ či „https“, pod kterým jsou definovaná a dostupná určitá data v rámci procesu ověřování identity. např. *http://specs.nic.cz/attr/contact/valid*

•**Identita** – Soubor dat o uživateli, které jsou vázané na identifikátor a jsou spravované poskytovatelem OpenID

•**Poskytovatel služeb** – Provozovatel webové aplikace (či přeneseně samotná aplikace, protože vše je řešeno automaticky bez manuálních zásahů), která požaduje ověření uživatelovy identity pomocí mojeID.

•**OpenID poskytovatel (OP)** – Zřizovatel a správce OpenID identit, na jehož webu dochází k autentizaci. V případě mojeID vždy CZ.NIC.

•**Jméno identity** – Jméno mojeID identity ve tvaru jmeno.mojeid.cz, které uživatel uvede do přihlašovacího formuláře jako identitu, pod kterou se chce přihlásit, např. *jnovakova.mojeid.cz*

•**Prohlášený identifikátor** – Identifikátor vzniklý ze jména identity, pod kterým je tato identita dostupná u OpenID poskytovatele a odkud lze získat metadata k tomuto identifikátoru. Např. https://*jnovakova.mojeid.cz/#nCHFlOoqQL*

•**Koncový bod OP** – URL adresa, na které poskytovatel OpenID přijímá zprávy. V případě mojeID je to vždy: *https://mojeid.cz/endpoint/*

3 Seznámení s mojeID

3.1 Základní principy mojeID

MojeID je služba, která dovoluje uživatelům zřídit si a centrálně spravovat svoji internetovou identitu (soubor osobních údajů - například jméno, příjmení, emailová adresa, telefon a další, doplněný o přihlašovací metody a údaje). S takovou identitou se pak uživatelé mohou přihlašovat na libovolných externích webových aplikacích (aplikací jiných poskytovatelů služeb než je poskytovatel identit), přičemž si nemusí vytvářet nové účty a opakovaně u nich vyplňovat základní informace a používat různá přihlašovací jména a hesla.

Služba mojeID je konkrétní implementací standardu OpenID ve verzi 2.0 pro decentralizovanou správu internetových identit, který definuje, jak se tyto centrálně spravované identity ověřují a jak vypadají jejich identifikátory.

> Oficiální specifikaci OpenID protokolu naleznete na: http://openid.net/developers/specs

MojeID je specifické pro prostředí českého internetu a nabízí poskytovatelům služeb další výhody oproti standardnímu OpenID, například rozšířenou sadu osobních údajů v identitách a jejich předávání, více přihlašovacích metod s možností požadovat určitou úroveň autentizace apod.

3.2 MojeID identita

Uživatelé si při zakládání identity musí zvolit jméno své identity, které jednoznačně určuje každou mojeID identitu a které má vždy tvar:

`jmeno.mojeid.cz` (např. `jnovakova.mojeid.cz`)

Toto jméno pak uživatelé používají pro přihlašování na stránkách poskytovatelé služeb – vkládají jej do příslušného přihlašovacího políčka. MojeID identita pak obsahuje:

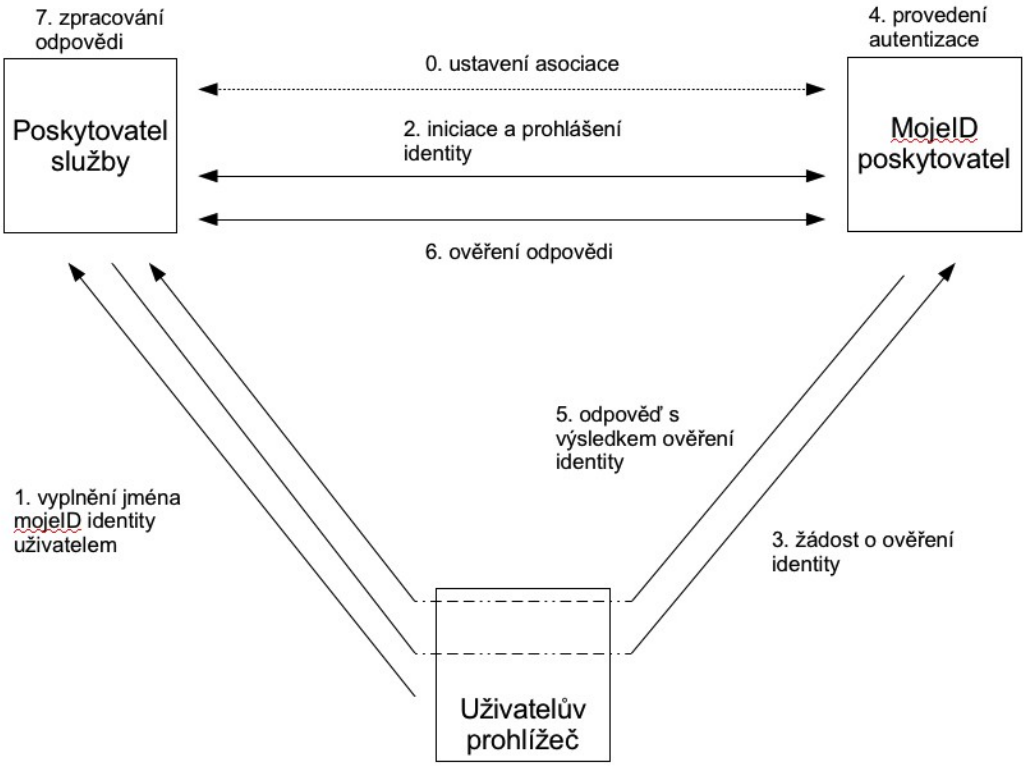
•údaje, které o sobě uživatel do identity uvede (běžné osobní údaje jako jméno, adresa, telefon, nickname, apod.)

•údaje, které jsou o uživateli poskytovány provozovatelem služby mojeID – sdružením CZ.NIC (zejména informace o fyzickém ověření identity resp. vybraných osobních údajích uživatele tzv. validaci či údaj o tom zda je osoba starší 18 let)

> Konkrétní výčet možných údajů v mojeID identitě naleznete v kapitole 4.4

3.3 Proces komunikace přes mojeID

Proces přihlášení pomocí mojeID se skládá z několika kroků, viz následující schéma.



1.**Ustavení asociace** – Dohodnutí sdíleného tajemství, pomocí kterého se budou ověřovat zprávy od *poskytovatele OpenID*.

2.**Vyplnění jména mojeID identity** – Uživatel přijde na stránku *poskytovatele služeb*, která podporuje mojeID. Tam vyplní *jméno identity* a klikne na tlačítko přihlásit.

3.**Iniciace** – V rámci iniciace se získá *prohlášený identifikátor* a další metadata o identitě a *poskytovateli OpenID* zejména *koncový bod OP*.

4.**Žádost o ověření identity** – *Poskytovatel služeb* sestaví žádost o ověření identity a tu nepřímo skrze přesměrování uživatelova prohlížeče odešle na *koncový bod poskytovatele OpenID*, kde se uživatel autentizuje.

5.**Provedení autentizace** – Uživatel se na přihlašovací stránce mojeID přihlásí pomocí některé z přihlašovacích metod – v současnosti je podporováno heslo a digitální certifikát a tím je jeho identita ověřena.

6.**Odpověď s výsledkem ověření identity** – Pokud o to *poskytovatel služeb* v žádosti o ověření identity požádá, je uživatel přesměrován zpět na stránky *poskytovatele služeb* a přes uživatelův prohlížeč je mu předána odpověď s výsledkem ověření identity.

7.**Ověření odpovědi** – Každá zpráva, kterou *poskytovatel služeb* obdrží od *poskytovatele OpenID* nepřímo přes uživatelův prohlížeč musí být ověřena, zda

opravdu pochází od *poskytovatele OpenID* a nebyla změněna. To se udělá buď pomocí asociace, viz bod 0 (ve valné většině případů), nebo se musí o toto ověření požádat.

8.**Zpracování odpovědi** – Na základě toho zda se jedná o úspěšné či neúspěšné přihlášení musí aplikace *poskytovatele služeb* reagovat a případně zpracovat další data, která jsou z této odpovědi získána.

4 Implementace podpory mojeID

V této sekci se seznámíte s technickými aspekty implementace služby mojeID do webových aplikací. Znalost tohoto textu není nezbytná k implementaci, ale je doporučená pro dobré a přesné porozumění principů a procesů fungování mojeID/OpenID. Většinu toho co, zde bude popsáno, vyřeší dostupné knihovny pro implementaci OpenID, které doporučujeme využívat. Pokud chcete rovnou začít s implementací, přejděte přímo na dokument pro specifický programovací jazyk či webovou technologii.

4.1 Ustavení asociace

Zprávy, které *poskytovatel služeb* obdrží nepřímo přes uživatelův prohlížeč od *poskytovatele OpenID* jsou digitálně podepsány. U každé takové zprávy je nutné podpisy ověřit a ujistit se, že opravdu pochází od *poskytovatele OpenID*. Je pro to možné využít dvou různých možností – tzv. stavovou a bezstavovou komunikaci mezi *poskytovatelem služeb* a *poskytovatelem OpenID*. Při **bezstavové** komunikaci musí *poskytovatel služeb* ověřit zprávu navázáním komunikace s *poskytovatelem OpenID* se žádostí o ověření konkrétní zprávy. To je náročnější na výkon a čas. **Stavová** komunikace začíná dohodnutím sdíleného tajemství ještě před začátkem samotného procesu přihlašování uživatele resp. ověřování identit – tzv. ustavení asociace. Toto sdílené tajemství má platnost nejdéle 14 dní a po jeho expiraci je nutné ustanovit asociaci znovu. Obě strany (*poskytovatel OpenID* i *poskytovatel služeb*) mohou také kdykoliv během platnosti sdíleného tajemství prohlásit toto sdílené tajemství za neplatné a i v tomto případě je pak potřeba ustanovit asociaci znovu, tak aby nebylo nutné používat bezstavovou komunikaci.

> OpenID knihovny, které je možné pro implementaci mojeID využít mohou používat obě možnosti. Pro běžné podmínky, doporučujeme používat stavovou komunikaci v co největší míře. V některých případech je nutné použít i bezstavovou komunikaci např. pokud sdílené tajemství vypršelo nebo jej jedna ze stran zneplatnila, je nutné zprávy ověřovat bezstavovou komunikací do doby než je ustavena nová asociace.

4.2 Vyplnění jména mojeID identity

Proces ověřování uživatelovy identity začne tím, že na stránkách *poskytovatele služeb* uživatel potvrdí požadavek na přihlášení s použitím mojeID. Pro maximální uživatelskou přívětivost stačí pouze tlačítko pro přihlášení, viz následující obrázky. Uživatelské jméno uživatel zadá na serveru mojeID.

Tlačítko pro přihlašování přes mojeID.

Vlastní dialog pro vložení mojeID identifikátoru.

Přihlašování ke službě mojeID je kompatibilní, jak s předchozí doporučenou verzí přihlašování se zadáním jména identity u poskytovatele služeb, tak se standardními způsoby přihlašování přes OpenID.

4.3 Iniciace

Aby *poskytovatel služby* mohl odeslat žádost o ověření identity, musí u většiny knihoven uvést buď identifikátor uživatele, nebo koncový bod OP. Pokud poskytovatel služeb nezná identifikátor uživatele (např. znovuověření uživatele) uvede místo něj koncový bod OP.

Pokud poskytovatel služeb zná identifikátor uživatele, získá jeho pomocí metadata o uživatelově identitě a o OpenID poskytovateli včetně *koncového bodu OP*. Na identifikátor uživatele se pošle HTTP požadavek a v těle stránky, která je tímto požadavkem získána se nachází mimo jiné i:

• *Prohlášený identifikátor* uživatele – Výsledné URL, z něhož se vrátilo tělo stránky s metadaty.

• *Vnitřní identifikátor* uživatele – Od *jména identity* se liší tím, že jde o *identifikátor*, který má tvar https://mojeid.cz/id/__hash__/, kde __hash__ je unikátní identifikace uživatele v systému mojeID např. https://mojeid.cz/id/nCzFlOhqQU/. Tuto vnitřní identitu je pak potřeba v dalších fázích přihlašovacího procesu kontrolovat, neboť to je identita, kterou rozpoznává *poskytovatel OpenID*, viz kapitola 4.7.

• *Koncový bod OP* – To je vždy https://mojeid.cz/endpoint/ a na tuto adresu budou směrovány žádosti o ověření identity.

4.4 Žádost o ověření identity

Jakmile *poskytovatel služeb* zná *koncový bod OP*, případně i *prohlášený identifikátor* a *vnitřní identifikátor* zasílá skrze přesměrování uživatelova prohlížeče žádost o ověření identity (o autentizaci). Žádost obsahuje speciální parametry pro její realizaci. Tyto parametry se uvádějí pomocí svých identifikátorů do těla zprávy. Konstrukci této žádosti o ověření identity opět přímo zajistí OpenID knihovny, které budete pro implementaci používat.

Žádost o ověření identity obsahuje obvykle následující parametry:

• ***Prohlášený identifikátor* uživatele, který bude ověřován** – *Jméno identity* odpovídající tomuto *prohlášenému identifikátoru* bude uživateli zobrazena na přihlašovací stránce mojeID. Chybí, pokud uživatel vybírá identifikátor u OP.

• **Návratovou adresu (URL) aplikace *poskytovatele služby*** – Na tuto adresu se vrátí uživatel po provedení přihlášení ze stránek *poskytovatele OpenID* a zde bude výsledek přihlašování aplikací *poskytovatelem služeb* zpracován. V naprosté většině případů bude tento parametr v žádosti uveden, jednou z mála speciálních situací je situace, kdy dochází k aktualizaci údajů v identitě, kdy už po provedení aktualizace není třeba návratu.

•**Oblast URL *poskytovatele služeb*** – Definuje část prostoru URL, pro niž je žádost o ověření identity platná. Návratová adresa *poskytovatele služeb* musí ležet v této oblasti URL. Na této nebo odpovídající adrese by měl být k dispozici XRDS dokument nebo zveřejněna jeho poloha.

•**Volba vyžadované přihlašovací metody** – Toho se dociluje umístěním identifikátoru příslušné přihlašovací metody do žádosti o ověření identity. Služba mojeID podporuje mimo běžného přihlašování heslem, přihlašováním pomocí digitálního certifikátu. Tuto metodu je možné vyžádat použitím identifikátoru:

http://schemas.openid.net/pape/policies/2007/06/phishing-resistant

•**Omezení doby přihlášení uživatele** – Pokud se uživatel úspěšně přihlásí k *poskytovateli služeb* systém mojeID udržuje „sezení“ tohoto uživatele po dobu jedné hodiny. Tedy pokud se uživatel v této době přihlašuje k jinému *poskytovateli služeb*, nemusí se na přihlašovací stránce mojeID znovu autentizovat. *Poskytovatel služeb* má ovšem možnost zkrátit pro svoji žádost o ověření identity na libovolnou menší dobu, pokud mu standardní doba přijde dlouhá např. z hlediska bezpečnosti. Tuto metodu je možné vyžádat použitím pole max_auth_age ve jmenném prostoru rozšíření PAPE -

http://specs.openid.net/extensions/pape/1.0

•**Požadované údaje z mojeID identity** – Do žádosti o ověření identity lze přidat i seznam jednotlivých údajů z mojeID identity, které aplikace poskytovatele služeb vyžaduje a které budou po úspěšném přihlášení a se souhlasem uživatele předány *poskytovateli služeb*. Pro každý údaj je nutné uvést jeho identifikátor. MojeID podporuje vyžádání následující údaje (podrobnosti a formáty jednotlivých položek lze nalézt přímo na uvedené adrese identifikátoru údaje; některé z těchto údajů – jméno, přezdívka, email, datum narození, PSČ a stát – lze získat jednodušším rozšíření Sreg):

Údaj	Identifikátor
Celé jméno	http://axschema.org/namePerson
Jméno	http://axschema.org/namePerson/first
Příjmení	http://axschema.org/namePerson/last
Přezdívka	http://axschema.org/namePerson/friendly
Jméno společnosti	http://axschema.org/company/name
Domácí adresa – Ulice	http://axschema.org/contact/postalAddress/home
Domácí adresa – Ulice2	http://axschema.org/contact/postalAddressAdditional/home
Domácí adresa – Ulice3	http://specs.nic.cz/attr/addr/main/street3
Domácí adresa – Město	http://axschema.org/contact/city/home
Domácí adresa – Stát	http://axschema.org/contact/state/home
Domácí adresa – Země	http://axschema.org/contact/country/home
Domácí adresa – PSČ	http://axschema.org/contact/postalCode/home
Faktur. adresa – Ulice	http://specs.nic.cz/attr/addr/bill/street
Faktur. adresa – Ulice2	http://specs.nic.cz/attr/addr/bill/street2
Faktur. adresa – Ulice3	http://specs.nic.cz/attr/addr/bill/street3
Faktur. adresa – Město	http://specs.nic.cz/attr/addr/bill/city
Faktur. adresa – Stát	http://specs.nic.cz/attr/addr/bill/sp
Faktur. adresa – Země	http://specs.nic.cz/attr/addr/bill/cc
Faktur. adresa – PSČ	http://specs.nic.cz/attr/addr/bill/pc
Doruč. adresa – Ulice	http://specs.nic.cz/attr/addr/ship/street
Doruč. adresa – Ulice2	http://specs.nic.cz/attr/addr/ship/street2

Doruč. adresa – Ulice3	http://specs.nic.cz/attr/addr/ship/street3
Doruč. adresa – Město	http://specs.nic.cz/attr/addr/ship/city
Doruč. adresa – Stát	http://specs.nic.cz/attr/addr/ship/sp
Doruč. adresa – Země	http://specs.nic.cz/attr/addr/ship/cc
Doruč. adresa – PSČ	http://specs.nic.cz/attr/addr/ship/pc
Koresp. adresa – Ulice	http://specs.nic.cz/attr/addr/mail/street
Koresp. adresa – Ulice2	http://specs.nic.cz/attr/addr/mail/street2
Koresp. adresa – Ulice3	http://specs.nic.cz/attr/addr/mail/street3
Koresp. adresa – Město	http://specs.nic.cz/attr/addr/mail/city
Koresp. adresa – Stát	http://specs.nic.cz/attr/addr/mail/sp
Koresp. adresa – Země	http://specs.nic.cz/attr/addr/mail/cc
Koresp. adresa – PSČ	http://specs.nic.cz/attr/addr/mail/pc
Telefon – Hlavní	http://axschema.org/contact/phone/default
Telefon – Domácí	http://axschema.org/contact/phone/home
Telefon – Pracovní	http://axschema.org/contact/phone/business
Telefon – Mobil	http://axschema.org/contact/phone/cell
Telefon – Fax	http://axschema.org/contact/phone/fax
Email – Hlavní	http://axschema.org/contact/email
Email – Notifikační	http://specs.nic.cz/attr/email/notify
Email – Další	http://specs.nic.cz/attr/email/next
URL – Hlavní	http://axschema.org/contact/web/default
URL – Blog	http://axschema.org/contact/web/blog
URL – Osobní	http://specs.nic.cz/attr/url/personal
URL – Pracovní	http://specs.nic.cz/attr/url/work
URL – RSS	http://specs.nic.cz/attr/url/rss
URL – Facebook	http://specs.nic.cz/attr/url/facebook
URL – Twitter	http://specs.nic.cz/attr/url/twitter
URL – LinkedIN	http://specs.nic.cz/attr/url/linkedin

IM -ICQ	http://axschema.org/contact/IM/ICQ
IM – Jabber	http://axschema.org/contact/IM/Jabber
IM – Skype	http://axschema.org/contact/IM/Skype
IM – Google Talk	http://specs.nic.cz/attr/im/google_talk
IM – Windows Live	http://specs.nic.cz/attr/im/windows_live
Identifikátor - ICO	http://specs.nic.cz/attr/contact/ident/vat_id
Identifikátor - DIC	http://specs.nic.cz/attr/contact/vat
Identifikátor – OP	http://specs.nic.cz/attr/contact/ident/card
Identifikátor - PAS	http://specs.nic.cz/attr/contact/ident/pass
Identifikátor - MPSV	http://specs.nic.cz/attr/contact/ident/ssn
Příznak - Student	http://specs.nic.cz/attr/contact/student
Příznak – Validace	http://specs.nic.cz/attr/contact/valid
Stav účtu	http://specs.nic.cz/attr/contact/status
Příznak – Starší 18 let	http://specs.nic.cz/attr/contact/adult
Obrázek (base64)	http://specs.nic.cz/attr/contact/image

Nejdůležitější parametry, které může žádost o ověření identity obsahovat, shrnuje následující tabulka:

Parametr (klíč)	Popis (hodnota)
openid.ns	Určení použitého OpenID protokolu. *http://specs.openid.net/auth/2.0*
openid.claimed_id	Prohlášený identifikátor uživatele. *http://jnovakova.mojeid.cz/*
openid.identity	Vnitřní identifikátor uživatele *http://mojeid.cz/id/unikatni_retezec/*
openid.assoc_handle	Identifikační řetězec dříve navázané asociace. *{HMAC-SHA256}{4c486ac3}{Ze6JZA==}*
openid.return_to	Návratová adresa z MojeID. Ve starších specifikacích protokolu OpenID se toto pole označuje openid.trust_root. *http://www.poskytovatel-sluzeb.cz/MojeID-Navrat.html*
openid.realm	Oblast URL poskytovatele služeb http://www.poskytovatel-sluzeb.cz/
openid.ns.ax	Určení rozšíření pro výměnu atributů. Řetězec „ax“ může být jakékoliv jiné pojmenování, které si zvolí vaše knihovna. Zde se pouze řekne, jak se na něj bude dále odkazovat. *http://openid.net/srv/ax/1.0*

`openid.ax.mode`	Režim výměny atributů (získání, uložení). *fetch_request*
`openid.ax.type.firstName`	Pojmenování atributu, který je *Poskytovatelem služeb* žádán. Opět může být libovolný řetězec. Jde o to zbavení se URL pro potřebu odkazování se na tento atribut. *http://axschema.org/namePerson/first*
`openid.ax.type.validated`	Další atribut – tentokrát informace o ověření uživatelových údajů. *http://specs.nic.cz/attr/contact/valid*
`openid.ax.type.jabber`	*http://axschema.org/contact/IM/Jabber*
`openid.ax.required`	Seznam atributů, o kterých *poskytovatel služeb* tvrdí, že jsou nezbytné pro řádné založení/aktualizaci účtu resp. pro fungování aplikace *poskytovatele služeb* samotné. *firstName,validated*
`openid.ax.if_available`	Seznam dodatečných atributů. *Poskytovatel služeb* by si je přál, ale nevadí, pokud je nedostane. *Jabber*
`openid.ns.pape`	Určení rozšíření pro autentizační politiky. http://specs.openid.net/extensions/pape/1.0
`openid.pape.max_auth_age`	Počet sekund, které určují stáří poslední proběhlé autentizace. Pokud se uživatel ještě neověřoval, anebo ověřoval, ale nevejde se do limitu, musí se autentizovat znovu. *3600*
`openid.pape.preferred_auth_policies`	Mezerou oddělený seznam identifikátorů požadovaných politik. *http://schemas.openid.net/pape/policies/2007/06/phishing-resistant*

4.5 Provedení autentizace

V okamžiku, kdy uživatel dorazí s žádostí o ověření identity od *poskytovatele služeb* na *koncový bod OP*, je mu zobrazena přihlašovací stránka, kde proběhne samotné přihlášení. Tato autentizace je provedena *poskytovatelem OpenID*. V rámci tohoto ověření se poskytovatel OpenID pokusí provést maximum úkonů, které byly specifikovány pomocí parametrů v žádosti o ověření identity. Celý proces se odehrává v systémech *poskytovatele OpenID* a z hlediska poskytovatele služeb nevyžaduje žádnou činnost.

Součástí je ověření návratové adresy *poskytovatele služeb*, uživatel je o výsledku tohoto ověření informován. V rámci tohoto ověření jsou získána data o *poskytovateli služeb* pomocí protokolu YADIS a ta jsou následně ověřena oproti údajům ve zprávě. Korektní *poskytovatel služeb* na dotaz z protokolu YADIS vrátí buď XRDS dokument nebo HTML dokument, v němž bude zveřejněna poloha XRDS dokumentu.

Poloha XRDS dokumentu se zveřejňuje následující značkou META v hlavičce:

```
<meta http-equiv="x-xrds-location"
    content="http://www.poskytovatel-sluzeb.cz/xrds.xml" />
```

XRDS dokument pak obvykle vypadá následovně

```
<?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>http://www.poskytovatel-sluzeb.cz/MojeID-Navrat.html</URI>
    </Service>
  </XRD>
</xrds:XRDS>
```

kde ve značce URI musí být návratová adresa *poskytovatele služeb* z žádosti o ověření identity. Během celého procesu k získání dokumentu nesmí server poskytovatele služeb vrátit přesměrování (HTTP kód 3xx), jinak je dokument považován za neplatný/podvržený.

V případě, že se nepodaří ověřit návratovou adresu *poskytovatele služeb*, je zobrazena uživateli některá z následujících zpráv:

–Pokud se nepodařilo spojit se s poskytovatelem služeb - `Nelze ověřit důvěryhodnost služby, kam se přihlašujete přes mojeID. Buďte zvláště obezřetní při předávání údajů z mojeID této službě. - We can not validate authenticity of the service where you want to login with mojeID. Use extra caution when handing over the data from mojeID.`

–Pokud se podařilo spojit se s poskytovatelem služeb, ale ověření návratové adresy selhalo - `Tento požadavek na přihlášení přes mojeID o sobě tvrdí, že přichází z jiné stránky, než tomu ve skutečnosti je. Zvažte, zda vůbec chcete pokračovat s předáváním údajů z vašeho mojeID. - This mojeID login request claims to be from other site than it really is. Consider carefully whether you want to continue with handing over the data from your mojeID.`

- Pokud oblast URL poskytovatele služeb nelze zpravovat v mojeID - `Tato oblast URL není dobře definovaná a nelze k ní nastavit důvěru. - This realm is not sane and thus you can not set trust for it.`

4.5.1 Výběr vhodné Oblasti URL poskytovatele služeb

Oblasti URL je v systému mojeid jednoznačným identifikátorem poskytovatele služeb, jeho správná volba tedy usnadní orientaci uživatelům. Dle specifikace OpenID by měla oblast URL odpovídat části URL prostoru, po níž je požadavek platný. V případě přihlašování by tedy oblast URL neměla být menší než je část URL prostoru, která je pokrytá následně vzniklou session.

Z tohoto plyne naše doporučení používat právě jeden realm na jednu doménu druhého řádu. Protože dvě URL, které se liší byť jen schématem, jsou dle specifikací rozdílné, velmi doporučujeme použití výhradně HTTPS v případě, že je dostupné. Tím se také zabrání odposlechu dat uživatelů, během jejich odesílání poskytovateli služeb.

Pokud používáte pouze jedinou doménu druhého řádu, pak doporučujeme zvolit oblast URL ve tvaru `https://nic.cz/` nebo `https://www.nic.cz/`. Zde

je třeba upozornit, že návratová adresa musí mít stejnou doménu jako realm, jinak je OpenID požadavek neplatný.

Pokud používáte poddomény třetích a nižších řádů, doporučujeme využít náhražkový znak * a zvolit oblast URL ve tvaru `https://*.nic.cz`. Tato oblast URL umožňuje používat návratové adresy s libovolnou poddoménou (ale ne s doménou samotnou v tomto případě `https://nic.cz/`) např. `https://www.nic.cz/`, `https://enum.nic.cz/navratova/adresa/`, `https://pod.do.me.na.nic.cz/`. XRDS dokument se bude hledat na URL, kde se znak * nahradí za "www".

4.6 Odpověď s výsledkem ověření identity

V případě, že o to *poskytovatel služby* požádal, je mu opět nepřímo přes přesměrování uživatelova prohlížeče zaslána zpět zpráva s odpovědí resp. výsledkem ověřování identity a dalšími daty, které si vyžádal. Tato odpověď má opět formu HTTP zprávy, přičemž v těle této zprávy jsou uvedena jednotlivá data vyjadřující jednotlivé informace výstupu z procesu ověření identity.

Následuje výčet nejdůležitějších polí odpovědi na žádost o ověření identity:

Klíč	Popis
`openid.claimed_id`	Vrací prohlášený identifikátor uživatele, od výchozího se může lišit fragmentem. Tento řetězec použije poskytovatel služeb k párování dat specifických pro uživatele. Je důležité při porovnávání dbát zřetel na všechny části řetězce včetně schématu a fragmentu. *https://jnovakova.mojeid.cz/#unikatni_retezec*
`openid.op_endpoint`	MojeID endpoint URL *https://mojeid.cz/endpoint/*
`openid.response_nonce`	Unikátní značka odpovědi. Žádné dvě odpovědi nemají stejnou – slouží k obraně před znovu odesláním odpovědi (tzv. replay attack). *2010-07-22T16:13:08ZiEnTtR*
`openid.signed`	Seznam polí, která jsou podepsána podpisem, viz následující klíč. *assoc_handle,claimed_id,ns,op_endpoint,pape.auth_policies,response_nonce,signed*
`openid.sig`	Podpis vyjmenovaných polí pro ověření pravosti. *hdtOpg3jCup1n6+elCXn+yLZAYc=*
`openid.ax.type.firstName`	Mapování oficiálního URL identifikátoru na řetězec používaný ve zprávě. *http://axschema.org/namePerson/first*
`openid.ax.value.firstName`	Hodnota atributu identity pro uvedený řetězec. *Jana*
`openid.pape.auth_policies`	Mezerou oddělený výčet přihlašovacích politik, které byly ve skutečnosti aplikovány. *http://schemas.openid.net/pape/policies/2007/06/phishing-resistant*
`openid.pape.auth_time`	Čas kdy byla ověřena uživatelova identita na serveru (vždy v UTC). *2005-05-15T17:11:51Z*

4.7 Ověření odpovědi

Každá zpráva s odpovědí je digitálně podepsána a musí být ověřena. Ověřují se následující části zprávy:

•návratová URL – hodnota „openid.return_to“ musí souhlasit s URL, na kterou byl požadavek doručen. Všechny parametry této URL musí být obsaženy v http zprávě, již *poskytovatel služeb* obdržel.

•*prohlášený identifikátor* – metadata náležící k *prohlášenému identifikátoru* získaná během iniciace nebo opakováním části tohoto procesu musí souhlasit s údaji obsaženými ve zprávě – *prohlášený identifikátor*, vnitřní identifikátor (), *koncový bod OP* a verze protokolu.

•značka odpovědi – zpráva se stejnou značkou nebyla od tohoto *poskytovatele OpenID* ještě přijata.

•podpis – všechna pole, která musí být podepsána, jsou podepsána a podpis je platný. Podpis si buď *poskytovatel služeb* ověří sám ve stavové komunikaci, nebo o kontrolu podpisu požádá *poskytovatele OpenID*.

Pokud jsou všechny tyto podmínky splněny, pak je zpráva platná a bylo ověřeno, že prohlášený identifikátor náleží uživateli. Všechny části by ale měla zpracovat knihovna implementující protokol.

4.8 Zpracování odpovědi

Pokud je zpráva s odpovědí na žádost o ověření identity úspěšně ověřena, může aplikace *poskytovatele služeb* data, která obsahuje, zpracovat a dokončit tak proces přihlašování pomocí mojeID. Toto zpracování musí zajistit webová aplikace na návratové adrese, která byla obsažena v žádosti na ověření identity.

4.8.1 Výsledek přihlášení

Při zpracování výsledku přihlášení je potřeba ošetřit následující speciální situace týkající se úspěšného přihlášení:

•**První přihlášení uživatele** – Pokud se uživatel, který se úspěšně přihlásil, ve webové aplikaci *poskytovatele služeb* poprvé, je ve většině případů nutné aby mu poskytovatel služeb založil v této své aplikaci účet, kde budou udržována data získaná z mojeID identity a samozřejmě i veškerá další data specifická pro příslušnou aplikaci. Při zakládání účtu je doporučeno:

- využít data získaná z mojeID identity zcela místo vyplňování registračního formuláře, případně zobrazit uživateli v registračním formuláři pouze ta políčka, jejichž obsah nebyl získán z mojeID.

- seznámit uživatele s tím, jaká data z mojeID identity příslušná aplikace potřebuje a doporučit mu, že je vhodné, aby umožnil jejich předávání při každém přihlášení.

- **Opakované přihlášení versus přihlášení nového uživatele** – Při každém zpracování odpovědi je třeba kontrolovat prohlášenou identitu uživatele, protože se může stát, že dva různí uživatelé mají stejné *jméno identity* a to tak, že jedna osoba zruší svoji mojeID identitu (a uvolní tak příslušné *jméno identity*) a jiná osoba si založí identitu se stejným *jménem identity*. Tito uživatelé jsou pak rozlišeni pomocí hash části na konci URL *prohlášené identity*.

- **Přihlášení uživatele, který o to nepožádal přímo** – Aplikace *poskytovatele služby* může obdržet odpověď s úspěšným přihlášením i v případě, že o přihlášení tento uživatel nepožádal přímo v aplikaci příslušného *poskytovatele služeb*. Jde o normální situaci, která by neměla být považována za chybu – požadavek na přihlášení šel z jiných stránek než na, kterou se vrací data (v protokolu se neuchovává informace o aplikaci, jež vygenerovala zprávu, pokud poskytovatel služeb takovou informaci vyžaduje, musí si ji doplnit sám). Uživatel je si ovšem vždy díky upozornění na přihlašovací stránce mojeID vědom, ke které službě se přihlašuje a komu předává data.

Při zpracování výsledku přihlášení je potřeba ošetřit následující situace týkající se negativního výsledku přihlašování:

- **Zamítnutí žádosti o přihlášení** - Uživatel může po příchodu na přihlašovací stránku zamítnout žádost o přihlášení např. z důvodu, že jej sám neinicioval. Aplikace pak musí ošetřit tento stav.

- **Nemožnost okamžitého ověření** – *Poskytovatel služeb* může vynutit ověření identity bez kontaktu s uživatelem, pokud toto ověření není *poskytovatel OpenID* schopen poskytnout, vrátí se tento typ odpovědi znamenající, že je třeba provést klasické ověření uživatele. Některé knihovny tento stav nerozlišují od předchozího stavu.

- **Chyba v protokolu** – *Poskytovatel OpenID* vrátí tento typ zprávy, pokud je schopen určit návratovou adresu *poskytovatele služeb*, ale není schopen rozpoznat jiná pole ve zprávě, neboť obsahuje data, jež jsou v rozporu s protokolem. *Poskytovatel OpenID* MojeID vrací tento chyb zpráv, např. pokud mu je doručena zpráva s vnitřním identifikátorem, jež není schopen ověřit.

4.8.2 Údaje z mojeID identity

Pokud je využito dotazování na údaje z mojeID identity, je nutné ošetřit následující speciální situace:

•**Opakované přihlašování uživatele** – Při každém opakovaném přihlášení uživatele pomocí mojeID je potřeba zkontrolovat, zda data, která jsou uložena v interním účtu aplikace *poskytovatele služeb,* jsou shodná jako data, která byla v rámci přihlášení získána z mojeID identity uživatele. V případě že se liší, je potřeba aktualizovat data v interním účtu daty z mojeID identity – ta jsou totiž pravděpodobně aktuálnější.

•**Neobdržení požadovaných údajů** – Uživatel má možnost vždy ovlivnit jaké údaje budou či nebudou při přihlášení předávány *poskytovateli služeb*. Může se tedy stát, že aplikace *poskytovatele služeb* některé údaje vyžaduje a přesto je díky uživatelově volbě nedostane. Je doporučeno ošetřit tuto situaci, aby data, která aplikace požaduje, byla rozdělena na nutná pro fungování aplikace a nepovinná, bez kterých se aplikace obejde. Podle toho rozdělení je pak vhodné navrhovat konkrétní chování dotyčné aplikace u obou druhů. Speciální funkcionalitou, která na tomto závisí, je možnost přihlášení pouze pro validované (fyzicky ověřené) uživatele mojeID. Pak je tímto nutným údajem položka: `http://specs.nic.cz/attr/contact/valid`. Údaje, u kterých uživatel nepovolil předání *poskytovateli služeb,* nejsou v těle odpovědi uváděny – tj. jako by vůbec nebyly požadovány (z obsahu zprávy lze tyto případy oddělit - pokud údaj je vyžadován, ale není vrácena jeho hodnota, je stále vrácena jeho definice, k níž je přiložen údaj o celkovém počtu hodnot rovný nule).

Testovací server

Testovací instance s podrobnějšími výstupy v případě chyb je dostupná na následujících adresách

–Koncový bod https://mojeid.fred.nic.cz/endpoint/

–Přihlašovací obrazovka do profilu https://mojeid.fred.nic.cz/consumer/

–Profil https://mojeid.fred.nic.cz/editor/

–Registrační obrazovky

–https://mojeid.fred.nic.cz/registration/

–https://mojeid.fred.nic.cz/transfer/

–Koncové body pro motivační program

–https://mojeid.fred.nic.cz/registration/endpoint/

–https://mojeid.fred.nic.cz/transfer/endpoint/

Testovací instance používá serverový certifikát podepsaný CA CZ.NIC (http://www.nic.cz/files/nic/doc/CZ.NIC-cacert.pem). Tento certifikát je třeba zpřístupnit knihovně, již používáte pro HTTPS komunikaci.

Pro zpřístupnění certifikátu knihovně CURL v Ubuntu stačí přidat certifikát do adresáře /usr/local/share/ca-certificates s příponou .crt a spustit příkaz update-ca-certificates.