Technická dokumentace pro implementaci MojeID

Vydání 3.1.4

CZ.NIC, z. s. p. o.

23.04.2025

Obsah

Kapitola 1

Právní upozornění

Přehled

1.1 Omezení odpovědnosti

S výjimkou případů újmy způsobené úmyslně nebo hrubou nedbalostí, nebo újmy způsobené člověku na jeho přirozených právech, případně v maximální možné míře, ve které to umožňuje právní řád uživatele, nenese sdružení CZ.NIC v žádném případě odpovědnost za jakékoli přímé nebo nepřímé újmy vyplývající z užití (včetně instalace) služby MojeID, včetně, avšak nikoliv výlučně, újmy na pověsti či jméně, újmy vzniklé v důsledku přerušení práce, ztráty nebo poškození dat nebo jakékoliv újmy hospodářské povahy (např. ušlý zisk, nedosažení předpokládaných úspor a podobně).

Prosíme, vezměte na vědomí, že informace uvedené v této dokumentaci nemají povahu záruky, vyjádřené výslovně nebo vyplývající z okolností (implicitně), a to zejména záruky vhodnosti pro konkrétní účel či záruky použitelnosti v jiných právních řádech než je právní řád České republiky.

1.2 Ochrana osobních údajů

Služba MojeID byla vyvinuta v České republice a její politiky ochrany osobních údajů jsou v souladu s právní úpravou ochrany osobních údajů České republiky, včetně stanovisek Úřadu na ochranu osobních údajů. Před užitím služby MojeID mimo území České republiky se ujistěte, že politiky ochrany osobních údajů služby MojeID odpovídají požadavkům právních předpisů příslušné země.

1.3 Rozhodné právo a příslušnost soudu

Dokumentace k implementaci služby MojeID (a související dokumenty) se řídí a vykládá ve všech ohledech v souladu s českým právem. Veškeré spory nebo nároky vzniklé nebo související s užitím služby MojeID (nebo této dokumentace), vč. jejího výkladu, provádění, neplatnosti atd. budou s konečnou platností rozhodovány Rozhodčím soudem při Hospodářské komoře České republiky a Agrární komoře České republiky (dále jen „soud“) podle jednacího řádu tohoto soudu jedním rozhodcem jmenovaným předsedou tohoto soudu.

1.4 Podmínky užití loga MojeID

Sdružení CZ.NIC je vykonavatelem majetkových autorských práv k obrazovému označení – logu MojeID a jeho odvozených modalit. Sdružení CZ.NIC tímto uděluje oprávnění logo MojeID a jeho odvozené modality užít v souvislosti s implementací, užitím služby MojeID a její propagací či propagací sdružení CZ.NIC a jeho produktů, a to všemi obvyklými způsoby užití loga. Oprávnění logo MojeID a jeho odvozené modality užít je bezúplatné, nevýhradní, množstevně, územně neomezené a omezené časově ve vztahu k užití služby MojeID. Uživatel není povinen oprávnění užít logo MojeID a jeho odvozené modality využít. Bez souhlasu sdružení CZ.NIC nesmí být oprávnění užít logo MojeID a jeho odvozené modality postoupeno třetí osobě. Logo MojeID a jeho odvozené modality nesmí být zneužity k poškození dobrého jména sdružení CZ.NIC nebo použity v rozporu se zájmy sdružení CZ.NIC. Žádným způsobem nesmí být logo MojeID a jeho odvozené modality znevažovány či užívány nedůstojným způsobem. Logo MojeID a jeho modality musí být vyobrazeny tak, jak je uvedeno v grafickém manuálu[1] a pouze v tomto vyobrazení smí být užívány.

[1] https://www.mojeid.cz/cs/pro-poskytovatele/jak-zavest/#download

Kapitola 2

Úvod

Tento dokument obsahuje obecný úvod do principů a fungování služby MojeID. Naleznete zde také 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.

MojeID aktuálně nabízí dva autentizační protokoly, které je možné použít. Jsou to OpenID Connect (doporučeno) a SAML 2.0.

Tip: Pokud zatím žádný z těchto protokolů ve svém systému nevyužíváte, doporučujeme použít *OpenID Connect*.

Jedná se o nejnovější z nabízených protokolů a do jeho vlastností se tak promítají zkušenosti z používání ostatních protokolů. Jeho hlavními přednostmi jsou jednoduchost implementace a podpora mobilních platforem.

Samozřejmě pokud již ve svém systému máte implementován protokol SAML 2.0, je logickým krokem využít tentýž protokol i pro integraci s MojeID.

Kapitola 3

Terminologie

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

Poskytovatel služeb
: provozovatel webové aplikace (či přeneseně samotná aplikace, protože vše je řešeno automaticky bez manuálních zásahů), která požaduje ověření uživatelovy *identity* pomocí MojeID.

Plný přístup
: varianta nasazení služby MojeID u poskytovatele služeb, pro podrobnosti viz https://www.mojeid.cz/cs/pro-poskytovatele/varianty-ceny/.

Omezený přístup
: varianta nasazení služby MojeID u poskytovatele služeb, pro podrobnosti viz https://www.mojeid.cz/cs/pro-poskytovatele/varianty-ceny/.

Identita
: soubor dat o uživateli, které jsou vázané na *identifikátor* a jsou spravované poskytovatelem OpenID.

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

Realm
: oblast URL poskytovatele služeb definující část prostoru URL, pro níž je žádost o ověření identity platná.

OP
Poskytovatel OpenID
OpenID poskytovatel
: zřizovatel a správce OpenID2 identit, na jehož webu dochází k autentizaci. V případě MojeID vždy CZ.NIC.

OCP
Poskytovatel OpenID Connect
OpenID Connect poskytovatel
: zřizovatel a správce OpenID Connect identit, na jehož webu dochází k autentizaci. V případě MojeID vždy CZ.NIC.

Jméno identity
: jméno MojeID *identity* ve tvaru `jmenoidentity.mojeid.cz`, které uživatel uvede do přihlašovacího formuláře jako identitu, pod kterou se chce přihlásit, např. `demo.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://demo.mojeid.cz/#JeDineCny`.

Koncový bod OP
URL adresa, na které poskytovatel OpenID2 přijímá zprávy. V případě MojeID je to vždy `https://mojeid.cz/endpoint/`.

Registration Endpoint
adresa URL, na které je možné zaregistrovat nového poskytovatele služeb podle specifikace OpenID Connect Dynamic Client Registration[2].

Client ID
jednoznačný identifikátor služby využívající OpenID Connect. K jeho přidělení dojde v průběhu registrace a používá se při veškeré komunikaci přes OpenID Connect.

Client Secret
heslo, kterým se prokazuje autenticita poskytovatele služeb v souvislosti s jeho Client ID. Toto heslo je možné změnit se znalostí Registration Access Token.

Registration Access Token
token, kterým je autentizovaná jakákoliv změna údajů o službě, například Client Secret.

Authorization Endpoint
adresa URL, na kterou poskytovatelé služeb přesměrovávají uživatele za účelem příhlášení.

ID Token
obsahuje ujištění o úspěšně provedeném ověření totožnosti uživatele, jehož údaje jsou obsažené uvnitř ID Tokenu.

Access Token
token, kterým je autentizovaný požadavek na UserInfo Endpoint.

UserInfo Endpoint
adresa URL, na které je možné s využitím Access Token získat detailní údaje o uživateli, pokud nejsou přítomny v ID Tokenu.

Token Endpoint
adresa URL, na které je možné získat Access Token, případně Refresh Token, pokud nebyly získány přímo v odpovědi na autentizaci.

Refresh Token
token, který je možné použít pro získání údajů z UserInfo Endpoint i bez přítomnosti uživatele.

[2] https://openid.net/specs/openid-connect-registration-1_0.html

Kapitola 4

Seznámení s MojeID

Tato kapitola vás seznámí se základními principy služby MojeID, podobou identit MojeID a procesem komunikace přes podporované protokoly.

4.1 Základní principy MojeID

MojeID je služba, která dovoluje uživatelům zřídit si a centrálně spravovat svoji internetovou identitu (soubor osobních údajů, například jméno, příjmení, e-mailová 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 a OpenID Connect ve verzi 1.0 pro decentralizovanou správu internetových identit, které definují, jak se tyto centrálně spravované identity ověřují a jak vypadají jejich identifikátory.

Účet MojeID lze propojit s Národním bodem pro identifikaci a autentizaci (NIA), čímž se ověří identita uživatele, který tak získá přístup ke službám veřejné správy. Více informací naleznete v kapitole *Napojení MojeID na NIA* (str. 14).

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 nebo více přihlašovacích metod s možností požadovat určitou úroveň autentizace.

4.2 MojeID identita

Uživatelé si při zakládání identity musí zvolit jméno své identity, které jednoznačně určuje každou MojeID identitu a které má vždy tvar `jmenoidentity.mojeid.cz` (bez diakritiky!), např. `demo.mojeid.cz`.

Toto jméno pak uživatelé používají pro přihlašování na stránkách poskytovatele služeb.

MojeID identita obsahuje:

- Údaje, které o sobě uživatel do identity uvede (běžné osobní údaje jako jméno, adresa, telefon, přezdívka, apod.)
- Údaje, které jsou o uživateli poskytovány provozovatelem služby MojeID (zejména informace o fyzickém ověření identity, resp. vybraných osobních údajích uživatele tzv. validaci, či údaj o tom, zda je osoba starší 18 let.)

Tip: Konkrétní výčty údajů, které je možné z MojeID identity předat přes jednotlivé protokoly, obsahuje udaje-openid, *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62) a *Příloha č. 3 – Seznam údajů pro předání (SAML)* (str. 67).

4.3 Komunikace s MojeID

V této sekci jsou obecně popsány procesy komunikace, které probíhají při přihlašování uživatele MojeID ke službě, která podporuje daný protokol.

4.3.1 Proces komunikace přes OpenID Connect

Proces přihlášení pomocí MojeID je možný několika různými způsoby (podle různých schémat), které se skládají z několika kroků. Při implementaci je možné zvolit schéma(ta) podle vašich preferencí.

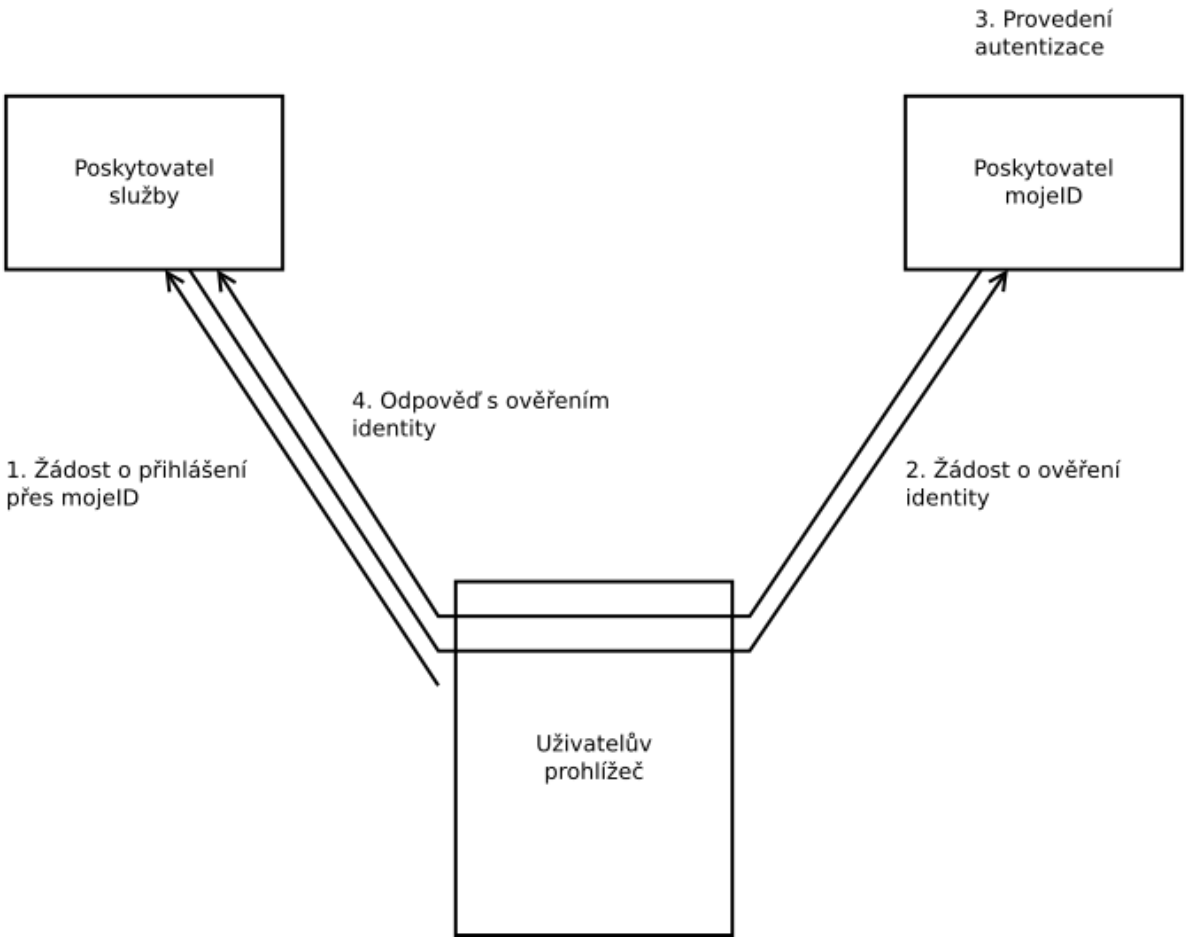
Počáteční kroky jsou společné pro všechna schémata:

0. **Registrace klienta** – Před použitím protokolu OpenID Connect je nutné registrovat svého klienta na serverech MojeID.
1. **Žádost o přihlášení přes MojeID** – Uživatel klikne na tlačítko „Přihlásit přes MojeID“.
2. **Žádost o ověření identity** – Poskytovatel služeb sestaví žádost o ověření identity a tu nepřímo skrze přesměrování uživatelova prohlížeče odešle na koncový bod poskytovatele (`Authorization Endpoint`) OpenID Connect, kde se uživatel autentizuje.
3. **Provedení autentizace** – Uživatel se na přihlašovací stránce MojeID přihlásí pomocí některé z přihlašovacích metod a tím je jeho identita ověřena. V současnosti je podporováno heslo, digitální certifikát, jednorázové heslo a bezpečnostní token (FIDO 2).

Další kroky závisí na zvoleném schématu:

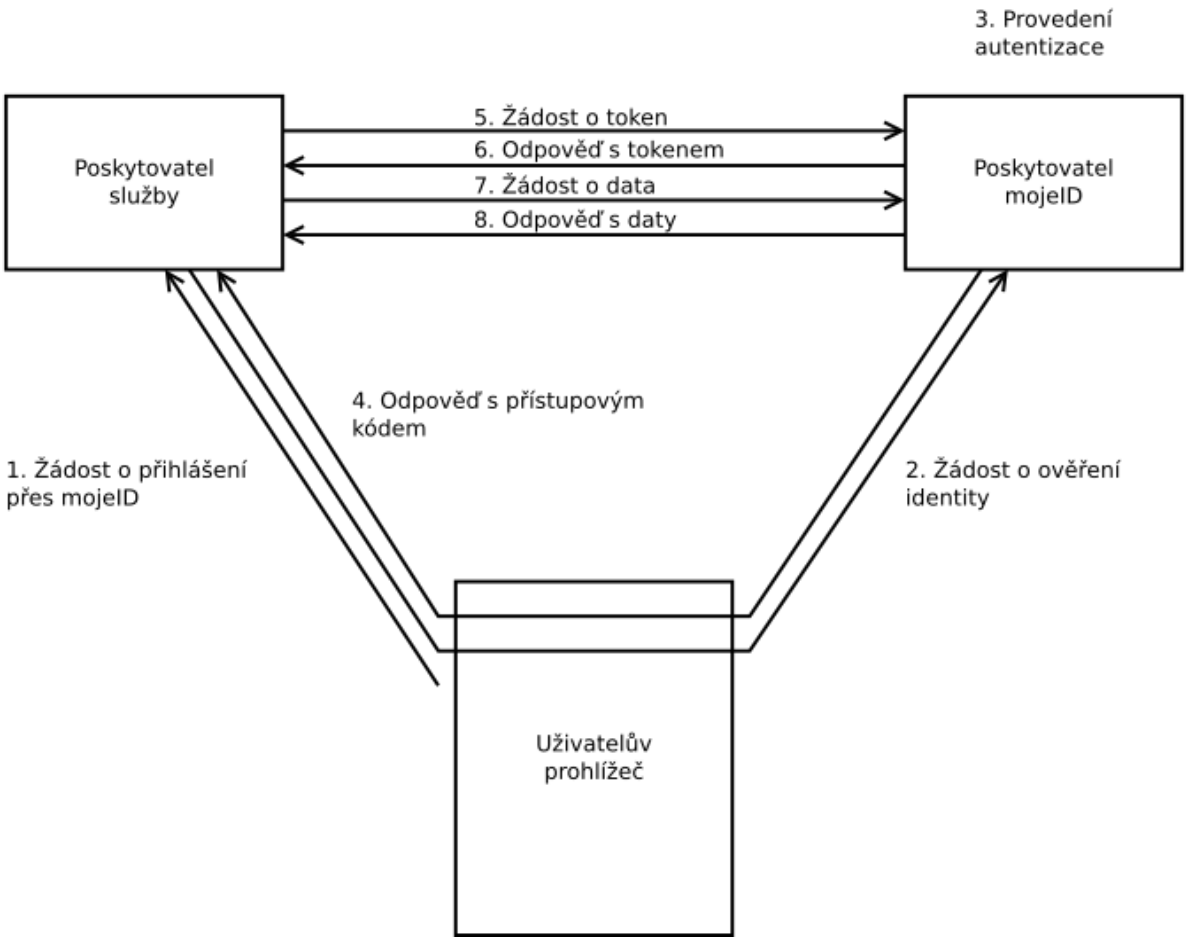
- *Implicitní schéma* (str. 9)
- *Přístupový kód* (str. 10)
- *Hybridní schéma* (str. 11)
- *Volba schématu* (str. 12)

Implicitní schéma



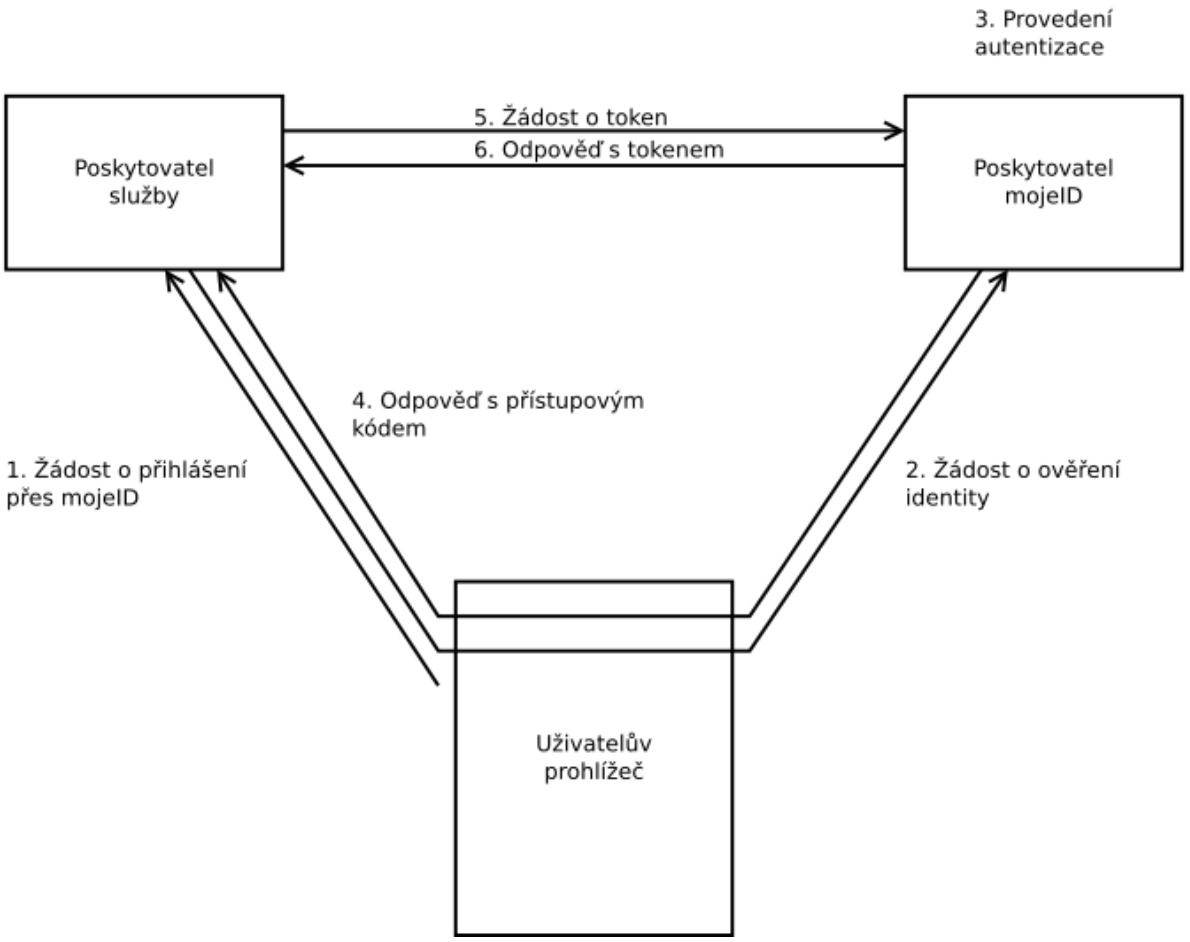
4. **Odpověd s výsledkem ověření identity** – Po přihlášení a potvrzení je uživatel přesměrován zpět na stránky poskytovatele služeb a prostřednictvím svého prohlížeče tak předá odpověď ze serverů MojeID s identifikátorem uživatele a ID tokenem. Pokud o to poskytovatel služeb v žádosti o ověření identity požádá, obsahuje ID token i data o uživateli.

Přístupový kód



4. **Odpověď s přístupovým kódem** – Po přihlášení a potvrzení je uživatel přesměrován zpět na stránky poskytovatele služeb a prostřednictvím svého prohlížeče tak předá odpověď ze serverů MojeID s přístupovým kódem.
5. **Žádost o token** – Poskytovatel služeb sestaví žádost o token, ve kterém použije právě získaný přístupový kód, a odešle ji na `Token Endpoint`.
6. **Odpověď s tokenem** – Poskytovatel služeb obdrží odpověď s přístupovým tokenem a ID tokenem
7. **Žádost o data** – Poskytovatel služeb sestaví žádost o uživatelská data s využitím získaného přístupového tokenu a odešle ji na `UserInfo Endpoint`.
8. **Odpověď s daty** – Poskytovatel služeb obdrží odpověď s daty uživatele.

Hybridní schéma



4. **Odpověď s přístupovým kódem** – Po přihlášení a potvrzení je uživatel přesměrován zpět na stránky poskytovatele služeb a prostřednictvím svého prohlížeče tak předá odpověď ze serverů MojeID s přístupovým kódem.
5. **Žádost o token** – Poskytovatel služeb sestaví žádost o token, ve kterém použije právě získaný přístupový kód, a odešle ji na `Token Endpoint`.
6. **Odpověď s tokenem** – Poskytovatel služeb obdrží odpověď s přístupovým tokenem a ID tokenem, který obsahuje data uživatele.

Volba schématu

Pro webové služby, které běží jen v prohlížeči („bez serveru“, např. JavaScript), je nejvhodnější *Implicitní schéma*.

Pro serverové služby je vhodnější schéma *Přístupový kód*, které poskytuje vyšší úroveň zabezpečení.

Následující tabulka shrnuje základní vlastnosti jednotlivých schémat a slouží jako pomůcka pro výběr vhodného schématu přihlášení.

Vlastnost	Implicitní schéma	Přístupový kód	Hybridní schéma
Všechny tokeny jsou vráceny z Authorization Endpoint	ano	ne	ne
Všechny tokeny jsou vráceny z Token Endpoint	ne	ano	ne
Tokeny nejsou viditelné v User Agent	ne	ano	ne
Klient může použít autentizaci	ne	ano	ano
Lze získat Refresh token	ne	ano	ano
Komunikace v jednom požadavku	ano	ne	ne
Většina komunikace probíhá server-to-server	ne	ano	různé

4.4 Favikona

Favikona je grafický prvek (ikona) asociovaný s určitou webovou stránkou nebo v případě MojeID službou. Webové prohlížeče umí zobrazit favikonu jako vizuální symbol identity webové stránky v adresním řádku, na záložkách nebo v oblíbených.

MojeID zobrazuje favikonu u názvu služby, ke které se uživatel MojeID přihlašuje, v přihlašovacím formuláři MojeID.

Použití favikony se liší podle protokolu.

4.4.1 Nastavení v OpenID Connect

Soubor favikony nahrajete na svůj web a jeho adresu nastavíte jako metadata (`logo_uri`) v registraci vašeho klienta, viz *Registrace klienta* (str. 35).

Pokud se na nastavené URI ikona nachází, pak je ve formuláři MojeID zobrazena, a to *bez ohledu* na typ přístupu (*plný/částečný*) služby k MojeID.

Obr. 1: Příklad zobrazení favikony

4.4.2 Nastavení pro SAML

Soubor favikony musíme explicitně nahrát do našeho systému.

Favikona se stahuje buď automaticky (1× týdně) nebo ji můžete dodat CZ.NICu přímo (např. e-mailem na adresu podpory) a my favikonu nahrajeme manuálně. Algoritmus při automatickém stahování hledá favikonu na *realmu* poskytovatele dle standardu W3C pro favikony[3], sekce *Method 1*.

Favikona nesmí být větší než 10 kB. Podporované formáty jsou ICO a PNG.

Zobrazení favikony u služeb komunikujících tímto protokolem je umožněno, jen pokud služba má *plný přístup*.

4.5 Napojení MojeID na NIA

Účet MojeID lze napojit na Národní bod pro identifikaci a autentizaci (NIA). Napojením se ověří identita uživatele, který tak získá přístup ke službám veřejné správy. Napojení účtu na NIA je možné pouze u fyzické osoby. Pokud je v účtu vyplněno pole `Organizace`, není napojení na NIA možné.

Předávané údaje ověřené přes NIA: `Křestní jméno`, `Příjmení`, `Adresa trvalého bydliště`, `Datum narození`. Takto ověřené údaje v účtu nelze měnit, jsou aktualizovány automaticky z registru obyvatel. Pokud chce uživatel uzamčené údaje upravit, musí zrušit napojení na NIA, čímž přijde o možnost přihlašování ke službám veřejné správy. Následnou úpravou údajů přijde i o ověření totožnosti.

MojeID podporuje dvě úrovně záruky dle eIDAS: „značná“ (substantial) a „vysoká“ (high). Poskytovatel si může vyžádat přihlášení takto ověřeným účtem pouze při použití protokolů SAML a OIDC.

Více informací, jak vyžádat takové přihlášení, naleznete v jednotlivých protokolech:

- OIDC: *Žádost o ověření identity účtem napojeným na NIA* (str. 46)
- SAML: *Žádost o ověření identity účtem napojeným na NIA* (str. 47)

[3] http://www.w3.org/2005/10/howto-favicon

Kapitola 5

Implementace podpory MojeID

Tato kapitola vás podrobněji provede jednotlivými fázemi komunikačního procesu, které je potřeba při implementaci podpory protokolu zohlednit, a prerekvizitami, které je potřeba pro funkční implementaci splnit.

Důležité: MojeID z bezpečnostních důvodů nedovoluje zobrazení přihlašovací stránky v rámcích (`<iframe>`).

5.1 Implementace pomocí OpenID Connect (OIDC)

V této sekci se seznámíte s technickými aspekty implementace služby MojeID pomocí protokolu OpenID Connect do webových aplikací.

Znalost tohoto textu je doporučená pro dobré a přesné porozumění principů a procesů fungování MojeID / OpenID Connect. Většinu toho, co zde bude popsáno, vyřeší *dostupné knihovny* (str. 16) pro implementaci OpenID Connect, které doporučujeme využívat.

Sekce *Přehled kroků implementace* (str. 32) vás provede procesem implementace krok za krokem. Další sekce se jednotlivými kroky zabývají více dopodrobna.

Oficiální specifikaci protokolu OpenID Connect naleznete na https://openid.net/specs/openid-connect-core-1_0.html.

Server MojeID zveřejňuje základní informace o konfiguraci OIDC na adrese https://mojeid.cz/.well-known/openid-configuration/.

Pro otestování implementace je vám k dispozici *Testovací instance MojeID* (str. 57).

Seznam údajů, které mohou být protokolem předány, (vč. jejich identifikátorů) obsahuje *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62).

Příklady a řešení chybových hlášek obsahuje *Příloha č. 6 – Příklady a řešení chybových hlášek* (str. 76).

Poznámka: Všechny dále uvedené příklady zdrojových kódů ilustrují implementaci v jazyce Python za použití knihovny `pyoidc`.

5.1.1 Přehled knihoven a modulů

Na oficiálních stránkách OpenID Foundation najdete seznam certifikovaných implementací protokolu OIDC v několika programovacích jazycích, viz Certified OpenID Connect Implementations[4]. Pro vás jsou zajímavé implementace pro *Relying Party*, která odpovídá poskytované službě.

Pro použití v mobilních aplikacích je vhodné využít knihovny pro nativní aplikace:

- pro Android např. http://openid.github.io/AppAuth-Android/,
- pro iOS např. http://openid.github.io/AppAuth-iOS/.

Dále je možné použít moduly pro nejpopulárnější platformy:

- *WordPress* (str. 16)
- *Joomla!* (str. 20)
- *PrestaShop* (str. 23)
- *OpenCart* (str. 25)
- *Drupal* (str. 27)
- Magento: OpenID Connect Single Sign-On (SSO) Magento Extension By Gluu[5]
- Moodle: OpenID Connect Authentication Plugin[6]
- Django: OIDC Django Packages[7]
- *MojeID login přes PHP klienta* (str. 30)

Pokud víte o nějakém dalším, který by tu neměl chybět, budeme rádi, když se s námi o tuto informaci podělíte (techsupport@mojeid.cz).

MojeID plugin pro WordPress

Důležité: Níže uvedený návod ještě dále testujeme. Budeme rádi, pokud se s námi podělíte o svoje zkušenosti s ním.

Instalace rozšíření

V administraci z repozitáře WordPress pluginů

1. V administraci WordPressu klikněte na záložku **Pluginy** a nahoře na stránce zvolte *Intalace pluginů*.
2. Vyhledejte plugin *OpenID Connect Generic Client* autora *daggerhart*, klikněte u něj na *Instalovat* a následně na *Aktivovat*. Dále postupujte podle *Registrace služby do MojeID* (str. 17).

[4] https://openid.net/developers/certified/
[5] https://github.com/GluuFederation/magento-oxd-extension
[6] https://moodle.org/plugins/auth_oidc
[7] https://djangopackages.org/grids/g/oidc/

V administraci pomocí instalačního balíčku

1. Stáhněte si **OpenID Connect Generic** plugin, který je dostupný na stránce WordPress pluginů[8] a na GitHubu[9].
2. V administraci WordPressu klikněte na záložku **Pluginy** a nahoře na stránce zvolte *Intalace pluginů*. Klikněte na tlačítko *Nahrát plugin*, zvolte stažený archiv a klikněte na *Instalovat*. Následně plugin aktivujte a postupujte podle *Registrace služby do MojeID* (str. 17).

Nahráním souborů na server (např. FTP/SCP)

1. Stáhněte si **OpenID Connect Generic** plugin, který je dostupný na stránce WordPress pluginů[10] a na GitHubu[11].
2. Stažený archiv extrahujte a celou složku přesuňte na server, na němž běží instance WordPressu, do složky `/wp-content/plugins/`.
3. V administraci WordPressu klikněte na záložku **Pluginy**, vyberte plugin *OpenID Connect Generic* a klikněte na tlačítko *Aktivovat*.
4. V záložce **Nastavení** vyberte *OpenID Connect Client* a poznamenejte si řetězec *Redirect URI*, který naleznete vespodu stránky.

Registrace služby do MojeID

Pokud registrujete testovací službu, přejděte na sekci *Registrace testovací služby* (str. 17). Pokud registrujete službu jdoucí do produkce, přejděte na sekci *Registrace produkční služby* (str. 18).

Registrace testovací služby

Více informací o testovací instanci MojeID lze najít v sekci *Testovací instance MojeID* (str. 57).

1. Jděte na úvodní stránku veřejné testovací instance MojeID[12] a za pomoci přítomného návodu si založte testovací účet.
2. Přejděte na adresu https://mojeid.regtest.nic.cz/consumer_admin/. Zde klikněte na tlačítko *Založení nové služby*.
3. Vyplňte položku *Název klienta* a do položky *Seznam URI pro přesměrování* vložte řetězec adresy *Redirect URI*, který jste si poznamenali v posledním kroku instalace rozšíření do WordPressu.
4. V rozbalovací nabídce položky *Přihlašovací metoda pro token endpoint* vyberte `Přihlašovací údaje v těle požadavku` a do políčka *Požadované typy odpovědí* vepište `code`. Následně klikněte na tlačítko *Uložit*.

[8] https://wordpress.org/plugins/daggerhart-openid-connect-generic/
[9] https://github.com/oidc-wp/openid-connect-generic/releases/latest
[10] https://wordpress.org/plugins/daggerhart-openid-connect-generic/
[11] https://github.com/oidc-wp/openid-connect-generic/releases/latest
[12] https://mojeid.regtest.nic.cz/index.html

5. Poznamenejte si řetězec znaků v poli *ID klienta* u služby, kterou jste právě vytvořili. Dále u služby klikněte na tlačítko *Aktualizovat* a poznamenejte si hodnotu položky *Tajemství klienta*.
6. Dále postupujte dle *Konfigurace rozšíření* (str. 18).

Registrace produkční služby

1. Založte si MojeID účet[13].
2. Přejděte na adresu https://mojeid.cz/consumer_admin/. Zde klikněte na tlačítko *Založení nové služby*.
3. Vyplňte položku *Název klienta* a do položky *Seznam URI pro přesměrování* vložte řetězec adresy *Redirect URI*, který jste si poznamenali v posledním kroku instalace rozšíření do WordPressu.
4. V rozbalovací nabídce položky *Přihlašovací metoda pro token endpoint* vyberte `Přihlašovací údaje v těle požadavku` a do políčka *Požadované typy odpovědí* vepište `code`. Následně klikněte na tlačítko *Uložit*.
5. Poznamenejte si řetězec znaků v poli ID klienta u služby, kterou jste právě vytvořili. Dále u služby klikněte na tlačítko *Aktualizovat* a poznamenejte si hodnotu položky *Tajemství klienta*.

Konfigurace rozšíření

1. V administraci WordPressu klikněte na záložku *Nastavení* a přejděte do sekce *OpenID Connect Client*. Zde vyplňte ID klienta, které jste získali během registrace služby, do pole *Client ID* a tajemství klienta do pole *Client secret*.
2. Vyplňte položku *OpenID Scope* v závislosti na tom, které informace po uživateli požadujete. Povinná je kategorie `openid`, pro přihlašování doporučujeme požadovat také `email`. Dalšími možnostmi jsou `profile phone address`, pro více informací navštivte dokumentaci OpenID Connect[14] a *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62).
3. Vyplňte adresy endpointů v závislosti na tom, zda jde o testovací instanci, nebo o instanci jdoucí do produkce:

   Konfigurace testovacích endpointů

   - **Login Endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/authorization/`
   - **Userinfo Endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/userinfo/`
   - **Token Validation Endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/token/`

[13] https://www.mojeid.cz/cs/zalozit-ucet/
[14] https://openid.net/specs/openid-connect-basic-1_0.html#Scopes

Konfigurace produkčních endpointů

- **Login Endpoint URL**: `https://mojeid.cz/oidc/authorization/`
- **Userinfo Endpoint URL**: `https://mojeid.cz/oidc/userinfo/`
- **Token Validation Endpoint URL**: `https://mojeid.cz/oidc/token/`

4. Nastavte hodnoty položek *Identity key, Nickname Key, Email Formatting* a *Display Name Formatting*. Jako *Identity Key* a *Nickname Key* doporučujeme použít `email` a možnost *Identify with User Name* nechat odškrtnutou.

> **Varování:** Do těchto položek můžete vyplnit pouze hodnoty, které si od uživatele vyžádáte v *OpenID Scope*. Nelze tedy například například nastavit formát jména, pokud v *OpenID Scope* nevznášíte požadavek na scope `profile`.

5. Odškrtněte políčko *Enable Refresh Token* a zaškrtněte *Link Existing Users*.
6. Nastavení uložte tlačítkem *Save Changes*.

Účty napojené na NIA[15]

Je-li účet napojen na NIA, jsou všechny osobní údaje (jméno, adresy atp.) ověřené. Toho lze využít například k povolení vkládání komentářů pod příspěvky pouze ověřeným uživatelům, povolení přístupu na určité stránky pouze zletilým osobám nebo zasílání pošty pouze na ověřené adresy.

Vzorová implementace využití NIA je k nalezení zde[16] v podobě pluginu, jenž automaticky schvaluje komentáře uživatelů, kteří jsou přihlášeni přes MojeID a mají svůj účet propojený se službami veřejné správy.

Důležité: Plugin slouží hlavně jako vzorová implementace a ukázka možností, jichž lze s MojeID dosáhnout. Neobsahuje tedy žádné WordPressové hooky, na které by se mohly napojovat další pluginy, a při implementaci je třeba buď tento plugin odpovídajícím způsobem upravit, nebo vytvořit vlastní.

Výzva k předávání údajů

V případě, že uživatel nepovolil předání nezbytných informací, jako je například `email`, a zaškrtl možnost *Předávat při každém přihlášení*, MojeID si tuto volbu zapamatuje a při každém dalším pokusu o přihlášení dojde k chybě kvůli nepředaným informacím. Pro tento účel můžete využít require prompt addon[17], který při každém přihlášení vyzve uživatele k potvrzení předávaných informací.

[15] https://info.identitaobcana.cz/ups/
[16] https://gitlab.nic.cz/utils/nia-approved-comment
[17] https://gitlab.nic.cz/utils/wordpress-openid-connect-require-prompt-addon

Poznámka: Tento problém může uživatel odstranit přihlášením do účtu MojeID a odstraněním služby v sekci *Nastavení > Předávání údajů*. Zde klikne na tlačítko - u příslušné služby a zvolí *Uložit*. Následně se může opět zkusit přihlásit a povolit předání všech potřebných informací.

Instalace addonu

- Stáhněte si require prompt addon[18].
- V adresáři WordPressu vytvořte složku `wp-content/mu-plugins/`, pokud již neexistuje. Přesuňte sem soubor `oidc-require-prompt-addon.php`.
- V nastavení OpenID Connect pluginu zaškrtněte možnost `Require prompt` a nastavení uložte.

Přihlášení pouze s účtem napojeným na NIA[Strana 20, 19]

Pokud chcete omezit okruh uživatelů, kteří se mohou přes MojeID přihlásit, pouze na ty, kteří mají svůj účet propojen s NIA, zadejte do pole `ACR values` řetězec `http://eidas.europa.eu/LoA/substantial`, kterým se vyžádá úroveň záruky „značná“. Pro více informací o úrovni záruky navštivte stránky *Napojení MojeID na NIA* (str. 14) a *Žádost o ověření identity účtem napojeným na NIA* (str. 46).

Poznámka: Řetězec skutečně odkazuje na protokol `http`, nikoli na `https`.

Chcete-li po uživateli pro přihlášení vyžadovat úroveň záruky „vysoká“[20], zaměňte hodnotu `substantial` za `high`. Pro běžné užití však úroveň „značná“ postačuje.

MojeID plugin pro Joomla

Důležité: Níže uvedený návod ještě dále testujeme. Budeme rádi, pokud se s námi podělíte o svoje zkušenosti s ním.

Instalace rozšíření

Stáhněte si OpenID Connect plugin[21]. V administraci Joomly přejděte do **System**, v kategorii *Install* zvolte *Extensions* a nahrajte sem stažený archiv.

[18] https://gitlab.nic.cz/utils/wordpress-openid-connect-require-prompt-addon
[19] https://info.identitaobcana.cz/ups/
[20] https://www.mojeid.cz/cs/podpora/uroven-vysoka/#vysoka-1
[21] https://gitlab.nic.cz/utils/joomla-openid-connect/-/releases/permalink/latest

Registrace služby do MojeID

Pokud registrujete testovací službu, přejděte na sekci *Registrace testovací služby* (str. 21). Pokud registrujete službu jdoucí do produkce, přejděte na sekci *Registrace produkční služby* (str. 21).

Registrace testovací služby

Více informací o testovací instanci MojeID lze najít v sekci *Testovací instance MojeID* (str. 57).

1. Jděte na úvodní stránku veřejné testovací instance MojeID[22] a za pomoci přítomného návodu si založte testovací účet.
2. Přejděte na adresu https://mojeid.regtest.nic.cz/consumer_admin/. Zde klikněte na tlačítko *Založení nové služby*.
3. Vyplňte položku *Název klienta*, do položky *Seznam URL pro přesměrování* vložte řetězec `http://example.com/index.php?option=com_openidconnect` a nahraďte v něm `example.com` svou vlastní doménou.
4. V rozbalovací nabídce položky *Přihlašovací metoda pro token endpoint* vyberte `Základní HTTP autentifikace` a do políčka *Požadované typy odpovědí* vepište `code`. Následně klikněte na tlačítko *Uložit*.
5. Poznamenejte si řetězec znaků v poli *ID klienta* u služby, kterou jste právě vytvořili. Dále u služby klikněte na tlačítko *Aktualizovat* a poznamenejte si hodnotu položky *Tajemství klienta*.

Registrace produkční služby

1. Založte si MojeID účet[23].
2. Přejděte na adresu https://mojeid.cz/consumer_admin/. Zde klikněte na tlačítko *Založení nové služby*.
3. Vyplňte položku *Název klienta*, do položky *Seznam URL pro přesměrování* vložte řetězec `http://example.com/index.php?option=com_openidconnect` a nahraďte v něm `example.com` svou vlastní doménou.
4. V rozbalovací nabídce položky *Přihlašovací metoda pro token endpoint* vyberte `Základní HTTP autentifikace` a do políčka *Požadované typy odpovědí* vepište `code`. Následně klikněte na tlačítko *Uložit*.
5. Poznamenejte si řetězec znaků v poli ID klienta u služby, kterou jste právě vytvořili. Dále u služby klikněte na tlačítko *Aktualizovat* a poznamenejte si hodnotu položky *Tajemství klienta*.

[22] https://mojeid.regtest.nic.cz/index.html
[23] https://www.mojeid.cz/cs/zalozit-ucet/

Konfigurace rozšíření

1. V administraci Joomly v záložce **System** zvolte *Global Configuration* a v postranní liště vyberte *OpenID Connect*.
2. Vyplňte ID klienta, které jste získali během registrace služby, do pole *Client ID* a tajemství klienta do pole *Client secret*.
3. Vyplňte adresy endpointů v závislosti na tom, zda jde o testovací instanci, nebo o instanci jdoucí do produkce:

   Konfigurace testovacích endpointů

   - **Authorization endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/authorization/`
   - **Token endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/token/`
   - **Userinfo endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/userinfo/`

   Konfigurace produkčních endpointů

   - **Authorization endpoint URL**: `https://mojeid.cz/oidc/authorization/`
   - **Token endpoint URL**: `https://mojeid.cz/oidc/token/`
   - **Userinfo endpoint URL**: `https://mojeid.cz/oidc/userinfo/`
4. Vyplňte položku *OpenID Scope* v závislosti na tom, které informace po uživateli požadujete. Povinná je kategorie `openid`, pro přihlašování doporučujeme požadovat také `email`. Dalšími možnostmi jsou `profile phone address`, pro více informací navštivte dokumentaci OpenID Connect[24] a *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62).
5. Volitelně zaškrtněte možnost *Require prompt*, která při každém přihlášení vyzve uživatele k potvrzení předávaných informací. Tato možnost se hodí v případě, že uživatel nepovolil předání nezbytných informací, jako je například `email`, a zaškrtl možnost *Předávat při každém přihlášení*. MojeID si tuto volbu zapamatuje a při každém dalším pokusu o přihlášení proto dojde k chybě kvůli nepředaným informacím.

   Poznámka: Tento problém může uživatel odstranit přihlášením do účtu MojeID a odstraněním služby v sekci *Nastavení > Předávání údajů*. Zde klikne na tlačítko - u příslušné služby a zvolí *Uložit*. Následně se může opět zkusit přihlásit a povolit předání všech potřebných informací.

   ---
6. Do kolonky *Post-login redirect URL* vyplňte **relativní** cestu stránky, na kterou má být uživatel po přihlášení přesměrován, například `index.php`.
7. Nastavení potvrďte tlačítkem *Save* navrchu stránky.

[24] https://openid.net/specs/openid-connect-basic-1_0.html#Scopes

Umístění tlačítka pro přihlášení

1. Stáhněte si balíček grafických prvků[25] a extrahujte jej.
2. V administraci Joomly otevřete v postranní nabídce položku **Content** a klikněte na tlačítko + vedle *Site Modules*.
3. Zvolte modul *Custom*. V editoru klikněte na tlačítko *CMS Content* a vyberte *Media*.
4. V okně *Media*, které se otevře, klikněte v horní části na *Upload* a nahrajte tlačítko pro přihlášení. Lze nahrát pouze obrázky formátu PNG. Toto tlačítko vyberte a klikněte na *Insert Media*.
5. Označte kliknutím obrázek, který jste vložili, v liště editoru rozklikněte menu (...) a zvolte ikonu linku (*Insert/Edit link*). Do pole URL vložte řetězec `https://example.com/index.php?option=com_openidconnect&task=login` a nahraďte v něm `example.com` svou vlastní doménou, volitelně můžete obrázek vycentrovat. Modul uložte kliknutím na *Save*.
6. V liště na pravé straně zvolte v rozbalovací nabídce *Position* umístění tlačítka.
7. Pokud chcete na stránce skrýt název modulu, přepněte přepínač *Title*. Pokud chcete název zobrazit, nazvěte modul `Přihlásit přes MojeID`. Nastavení uložte.

MojeID plugin pro PrestaShop

Důležité: Níže uvedený návod ještě dále testujeme. Budeme rádi, pokud se s námi podělíte o svoje zkušenosti s ním.

Instalace rozšíření

1. Stáhněte si OpenID Connect plugin[26].
2. V administraci PrestaShopu klikněte na záložku **Moduly** a vyberte *Správce modulů*. Klikněte na tlačítko *Nahrát modul* a v dialogovém okně zvolte stažený archiv. Následně zvolte možnost *Konfigurovat*.
3. Zkopírujte si řetězec *Redirect URL* z poslední kolonky na stránce. Záložku nezavírejte.

[25] https://www.mojeid.cz/cs/pro-poskytovatele/jak-zavest/#download
[26] https://gitlab.nic.cz/utils/prestashop-openid-connect/-/releases/permalink/latest

Konfigurace rozšíření

1. V otevřené záložce vyplňte ID klienta, které jste získali v minulém kroku, do pole *Client ID* a tajemství klienta do pole *Client secret*. Nepovinně můžete vyplnit i jméno služby.
2. Vyplňte adresy endpointů v závislosti na tom, zda jde o testovací instanci, nebo o instanci jdoucí do produkce:

   Konfigurace testovacích endpointů

   - **Authorization endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/authorization/`
   - **Token endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/token/`
   - **Userinfo endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/userinfo/`

   Konfigurace produkčních endpointů

   - **Authorization endpoint URL**: `https://mojeid.cz/oidc/authorization/`
   - **Token endpoint URL**: `https://mojeid.cz/oidc/token/`
   - **Userinfo endpoint URL**: `https://mojeid.cz/oidc/userinfo/`
3. Vyplňte položku *Scope* v závislosti na tom, které informace po uživateli požadujete. Povinná je kategorie `openid`, pro přihlašování doporučujeme požadovat také `email`. Dalšími možnostmi jsou `profile phone address`, pro více informací navštivte dokumentaci OpenID Connect[27] a *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62).
4. Volitelně zaškrtněte možnost *Require prompt*, která při každém přihlášení vyzve uživatele k potvrzení předávaných informací. Tato možnost se hodí v případě, že uživatel nepovolil předání nezbytných informací, jako je například `email`, a zaškrtl možnost *Předávat při každém přihlášení*. MojeID si tuto volbu zapamatuje a při každém dalším pokusu o přihlášení proto dojde k chybě kvůli nepředaným informacím.

   Poznámka: Tento problém může uživatel odstranit přihlášením do účtu MojeID a odstraněním služby v sekci *Nastavení* > *Předávání údajů*. Zde klikne na tlačítko - u příslušné služby a zvolí *Uložit*. Následně se může opět zkusit přihlásit a povolit předání všech potřebných informací.

   ---
5. Nastavení potvrďte tlačítkem *Uložit*.

[27] https://openid.net/specs/openid-connect-basic-1_0.html#Scopes

MojeID plugin pro OpenCart

Důležité: Níže uvedený návod ještě dále testujeme. Budeme rádi, pokud se s námi podělíte o svoje zkušenosti s ním.

Instalace rozšíření

1. Stáhněte si OpenID Connect plugin[28].
2. V administraci Opencartu přejděte do **Extensions**, v kategorii *Installer* klikněte na tlačítko *Upload* (šipka vzhůru) a nahrajte sem stažený archiv.
3. V seznamu *Installed Extensions* najděte plugin *OpenID Connect* a klikněte u něj na zelené tlačítko +.
4. V kategorii **Extensions** přejděte do *Extensions* a v rozbalovací nabídce *Choose the extension type* vyberte `Modules`.
5. V seznamu *Modules* najděte *OpenID Connect*, aktivujte jej kliknutím na zelené tlačítko + a vstupte do nastavení kliknutím na ikonu tužky.
6. Zkopírujte si řetězec *Redirect URL* vespodu stránky a záložku nezavírejte.

Konfigurace rozšíření

1. V otevřené záložce *OpenID Connect* vyplňte ID klienta, které jste získali během registrace služby, do pole *Client ID* a tajemství klienta do pole *Client secret*.
2. Vyplňte adresy endpointů v závislosti na tom, zda jde o testovací instanci, nebo o instanci jdoucí do produkce:

Konfigurace testovacích endpointů

- **Authorization endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/authorization/`
- **Token endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/token/`
- **Userinfo endpoint URL**: `https://mojeid.regtest.nic.cz/oidc/userinfo/`

Konfigurace produkčních endpointů

- **Authorization endpoint URL**: `https://mojeid.cz/oidc/authorization/`
- **Token endpoint URL**: `https://mojeid.cz/oidc/token/`
- **Userinfo endpoint URL**: `https://mojeid.cz/oidc/userinfo/`

[28] https://gitlab.nic.cz/utils/opencart-openid-connect/-/releases/permalink/latest

3. Vyplňte položku *OpenID Scope* v závislosti na tom, které informace po uživateli požadujete. Povinná je kategorie `openid`, pro přihlašování doporučujeme požadovat také `email`. Dalšími možnostmi jsou `profile phone address`, pro více informací navštivte dokumentaci OpenID Connect[29] a *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62).
4. Volitelně zaškrtněte možnost *Require prompt*, která při každém přihlášení vyzve uživatele k potvrzení předávaných informací. Tato možnost se hodí v případě, že uživatel nepovolil předání nezbytných informací, jako je například `email`, a zaškrtl možnost *Předávat při každém přihlášení*. MojeID si tuto volbu zapamatuje a při každém dalším pokusu o přihlášení proto dojde k chybě kvůli nepředaným informacím.

   Poznámka: Tento problém může uživatel odstranit přihlášením do účtu MojeID a odstraněním služby v sekci *Nastavení* > *Předávání údajů*. Zde klikne na tlačítko - u příslušné služby a zvolí *Uložit*. Následně se může opět zkusit přihlásit a povolit předání všech potřebných informací.

   ---

5. Nastavení potvrďte tlačítkem *Save* vespodu stránky.

Umístění tlačítka pro přihlášení

Tlačítko pro přihlášení pomocí MojeID musí být přidáno ručně do zdrojového kódu šablony stránky. Šablony můžete upravovat v záložce **Design** > *Theme Editor* > *commmon*.

Příklady implementace

Tlačítko v záhlaví stránky

Do šablony `header.twig` vložte mezi řádky 56 a 57 následující kód, v němž nahradíte `example.com` svou vlastní doménou:

```
<li><a href="http://example.com/index.php?route=extension%2Fopenidconnect
↪%2Fmodule%2Fopenidconnect.login" class="dropdown-item">Přihlásit přes MojeID
↪</a></li>
```

Důležité: Pokud jste již v šabloně dělali změny, číslo řádku se může lišit. Kód vložte do třídy `dropdown-menu dropdown-menu-right` mezi statementy `{%if not logged%}` a `{%else%}` a ujistěte se, že jej nevkládáte do jiné položky třídy `dropdown-item`. Těsně před Vámi vloženým kódem musí být html tag `</li>`.

---

[29] https://openid.net/specs/openid-connect-basic-1_0.html#Scopes

Tlačítko v zápatí stránky

Stáhněte si balíček grafických prvků[30] a obrázek tlačítka pro přihlášení nahrajte na server do složky `image` instance OpenCartu. Doporučujeme formát SVG.

Do šablony `footer.twig` vložte mezi řádky 43 a 44 následující kód, v němž nahradíte `example.com` svou vlastní doménou a `X` číslem obrázku, který chcete pro tlačítko použít:

```
{% if not logged %}
<li>
<a href="http://example.com/index.php?route=extension%2Fopenidconnect%2Fmodule
↪%2Fopenidconnect.login">
<img src="/image/mojeid_tlacitko_Prihlasit_0X.svg" width=70%></a>
</li>
{% endif %}
```

Důležité: Pokud jste již v šabloně dělali změny, číslo řádku se může lišit. Kód vložte do třídy `list-unstyled` a ujistěte se, že jej nevkládáte do jiné položky této třídy. Těsně před Vámi vloženým kódem musí být html tag `</li>`.

Poznámka: Příklad ilustruje implementaci tlačítka s českým nápisem. Pokud chcete použít tlačítko s anglickým nápisem, upravte odpovídajícím způsobem cestu zdroje obrázku.

MojeID plugin pro Drupal

Důležité: Níže uvedený návod ještě dále testujeme. Budeme rádi, pokud se s námi podělíte o svoje zkušenosti s ním.

Instalace rozšíření

1. Pomocí PHP composeru[31] nainstalujte OpenID Connect[32] plugin. Řiďte se přitom verzí PHP a Drupalu. Pro instalaci s Drupalem 10 a PHP 8.1 spusťte v kořenovém adresáři Drupalu příkaz `composer require 'drupal/openid_connect:^3.0@alpha'`. Pro jiné verze zvolte odpovídající příkaz na stránce pluginu.
2. V administraci Dupalu přejděte do sekce *Nastavení* a v kategorii *Uživatelé* zvolte **OpenID Connect**.

[30] https://www.mojeid.cz/cs/pro-poskytovatele/jak-zavest/#download
[31] https://getcomposer.org/
[32] https://www.drupal.org/project/openid_connect

Testovací instalace

Klikněte na tlačítko **+ Generic OAuth 2.0** a nastavte jméno služby, doporučujeme `MojeID`.

Produkční instalace

Pokud chcete pro svoji službu použít přednastavený scope informací, které budou po uživateli požadovány, klikněte na tlačítko **+ MojeID** a nastavte jméno služby, doporučujeme `MojeID`. Při konfiguraci pak postupujte dle sekce *Přednastavená konfigurace* (str. 30). Přednastaveny jsou hodnoty `openid profile email`.

Pokud chcete zvolit svůj vlastní scope, zvolte **+ Generic OAuth 2.0**, nastavte jméno služby a během konfigurace postupujte dle sekce *Pokročilá konfigurace* (str. 30).

3. Jméno potvrďte stisknutím klávesy Enter nebo kliknutím do prázdného místa na stránce.
4. Poznamenejte si řetězec *Redirect URL*, který naleznete vespodu stránky. Záložku s Drupalem nezavírejte.

Registrace služby do MojeID

Pokud registrujete testovací službu, přejděte na sekci *Registrace testovací služby* (str. 28). Pokud registrujete službu jdoucí do produkce, přejděte na sekci *Registrace produkční služby* (str. 29).

Registrace testovací služby

Více informací o testovací instanci MojeID lze najít v sekci *Testovací instance MojeID* (str. 57).

1. Jděte na úvodní stránku veřejné testovací instance MojeID[33] a za pomoci přítomného návodu si založte testovací účet.
2. Na nástěnce účtu[34] klikněte na tlačítko *Založení nové služby*.
3. Vyplňte položku *Název klienta* a do položky *Seznam URI pro přesměrování* vložte řetězec adresy *Redirect URL* z posledního kroku instalace rozšíření do PrestaShopu.
4. V rozbalovací nabídce položky *Přihlašovací metoda pro token endpoint* vyberte `Základní HTTP autentifikace` a do políčka *Požadované typy odpovědí* vepište `code`. Následně klikněte na tlačítko *Uložit*.
5. Poznamenejte si řetězec znaků v poli *ID klienta* u služby, kterou jste právě vytvořili. Dále u služby klikněte na tlačítko *Aktualizovat* a poznamenejte si hodnotu položky *Tajemství klienta*.
6. Dále postupujte dle *Konfigurace rozšíření* (str. 29).

[33] https://mojeid.regtest.nic.cz/index.html
[34] https://mojeid.regtest.nic.cz/consumer_admin/

Registrace produkční služby

1. Založte si MojeID účet[35].
2. Na nástěnce účtu[36] klikněte na tlačítko *Založení nové služby*.
3. Vyplňte položku *Název klienta* a do položky *Seznam URI pro přesměrování* vložte řetězec adresy *Redirect URL* z posledního kroku instalace rozšíření do PrestaShopu.
4. V rozbalovací nabídce položky *Přihlašovací metoda pro token endpoint* vyberte `Základní HTTP autentifikace` a do políčka *Požadované typy odpovědí* vepište `code`. Následně klikněte na tlačítko *Uložit*.
5. Poznamenejte si řetězec znaků v poli ID klienta u služby, kterou jste právě vytvořili. Dále u služby klikněte na tlačítko *Aktualizovat* a poznamenejte si hodnotu položky *Tajemství klienta*.

Konfigurace rozšíření

V otevřené záložce nastavení **OpenID Connect** vyplňte ID klienta, které jste získali během registrace služby, do pole *Client ID* a tajemství klienta do pole *Client secret*.

Pokud testujete funkčnost služby, postupujte podle návodu *Testovací konfigurace* (str. 29). Pokud zavádíte již otestovanou službu, postupujte dle *Přednastavená konfigurace* (str. 30), nebo dle *Pokročilá konfigurace* (str. 30).

Testovací konfigurace

1. Vyplňte adresy endpointů:
   - **Authorization endpoint**: `https://mojeid.regtest.nic.cz/oidc/authorization/`
   - **Token endpoint**: `https://mojeid.regtest.nic.cz/oidc/token/`
   - **UserInfo endpoint**: `https://mojeid.regtest.nic.cz/oidc/userinfo/`
2. Vyplňte položku *OpenID Scope* v závislosti na tom, které informace po uživateli požadujete. Povinná je kategorie `openid`, pro přihlašování doporučujeme požadovat také `email`. Dalšími možnostmi jsou `profile phone address`, pro více informací navštivte dokumentaci OpenID Connect[37] a *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62).
3. Nastavení potvrďte tlačítkem *Create OpenID Connect client*.

[35] https://www.mojeid.cz/cs/zalozit-ucet/
[36] https://mojeid.cz/consumer_admin/
[37] https://openid.net/specs/openid-connect-basic-1_0.html#Scopes

Přednastavená konfigurace

Pokud jste vybrali možnost **+ MojeID** a vyplnili jste položky *Client ID* a *Client secret*, není již potřeba žádná konfigurace, nastavení pouze potvrďte tlačítkem *Create OpenID Connect client*.

Pokročilá konfigurace

Pokud chcete nastavit jiný scope informací, které budou po uživateli požadovány, než je přednastaven v MojeID přihlášení, postupujte následovně:

1. Vyplňte adresy endpointů:
   - **Authorization endpoint**: `https://mojeid.cz/oidc/authorization/`
   - **Token endpoint**: `https://mojeid.cz/oidc/token/`
   - **UserInfo endpoint**: `https://mojeid.cz/oidc/userinfo/`
2. Vyplňte položku *OpenID Scope* v závislosti na tom, které informace po uživateli požadujete. Povinná je kategorie `openid`, pro přihlašování doporučujeme požadovat také `email`. Dalšími možnostmi jsou `profile phone address`, pro více informací navštivte dokumentaci OpenID Connect[38] a *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62).
3. Nastavení potvrďte tlačítkem *Create OpenID Connect client*.

Umístění tlačítka pro přihlášení

1. V administraci Drupalu vstupte do kategorie *Struktura* > *Umístění bloků*. Zde si zvolte umístění tlačítka pro přihlášení.
2. U příslušného umístění klikněte na tlačítko *Umístěte blok*, zvolte `OpenID Connect client` a klikněte na *Umístit blok*. Jako nadpis zvolte `Přihlásit přes MojeID` a nastavení uložte.
3. Vespodu stránky klikněte na tlačítko *Uložit bloky*.

Přihlášení k MojeID pomocí PHP klienta

Návod obsahuje postup instalace pluginu pro přihlášení k MojeID pomocí PHP klienta a příklad použití.

Prerekvizity

Než budete moci pokračovat, je třeba provést následující:

- Nainstalujte si Composer[39]
- Nainstalujte si Docker Engine[40]

[38] https://openid.net/specs/openid-connect-basic-1_0.html#Scopes
[39] https://getcomposer.org/
[40] https://docs.docker.com/engine/install/

- Stáhněte si plugin `php-mojeid-oidc` z našeho veřejného GitLabu[41]

Instalace

1. Ve složce s pluginem `php-mojeid-oidc` spusťte následující příkazy:

```
cd php
composer install

# vytvoření konfiguračního souboru pro konkrétní službu
cp config.{template,local}.php

# spuštění webového serveru
sudo docker compose -f ../docker/docker-compose.yml up
```

2. Proveďte ruční registraci klienta MojeID[42].
   - Do *seznamu URI* je třeba vyplnit URI, přes kterou Váš webový prohlížeč přistupuje k PHP aplikaci (složce `php` z tohoto příkladu). Při použití přiloženého dockerového řešení na vlastním počítači lze zadat `https://localhost:8443/`.
     - Adresu, se kterou webový server pracuje, můžete zjistit z metody `OpenIDConnectClient::getRedirectURL()`.
     - Pokud neodpovídá tomu, co potřebujete, nastavte správnou adresu metodou `OpenIDConnectClient::setRedirectURL()`.
3. V souboru `config.local.php` vyplňte požadované údaje:
   - `OPEN_ID_PROVIDER_URL` je základní URL služby, ke které se chcete připojit
   - `OPEN_ID_CLIENT_ID` je *ID klienta* ze stránky https://mojeid.regtest.nic.cz/consumer_admin/
   - `OPEN_ID_CLIENT_SECRET` je *Tajemství klienta* ze stránky s podrobnostmi dané služby
     - na výše uvedené stránce přejděte v příslušném řádku na odkaz *Aktualizovat*

Použití

1. Navštivte webovou stránku ukázky (https://localhost:8443/).
2. Po případném potvrzení certifikátu s vlastním podpisem budete přesměrováni na přihlašovací stránku MojeID.
3. Po prvním přihlášení budete vyzváni k souhlasu s předáním údajů.
4. Po potvrzení budete přesměrováni zpět na stránku naší aplikace, kde uvidíte křestní jméno zadaného uživatele (pokud jste udělili příslušný souhlas).

[41] https://gitlab.nic.cz/mojeID/plugins
[42] https://www.mojeid.cz/dokumentace/html/ImplementacePodporyMojeid/OpenidConnect/Registrace/index.html

Důležité: Uvedené moduly dále testujeme. Budeme rádi, pokud se s námi podělíte o svoje zkušenosti s nimi.

5.1.2 Přehled kroků implementace

Tento přehled obsahuje organizační a technické kroky, které musíte provést v rámci implementace přihlášení do vaší služby přes MojeID protokolem OpenID Connect. Jednotlivé kroky jsou pro přehlednost stručné a říkají, *co* je třeba udělat, zatímco cíle odkazů rozvádí, *jak* to udělat, nebo obsahují doplňující informace. Přehled může sloužit jako kontrolní seznam (*checklist*).

Příprava testovacího prostředí

1. *Zaregistrovat službu* (str. 35) (klienta) na *testovacím Registration Endpointu* (str. 58) – tím získáte testovací metadata svojí služby (*Client ID*, *Client Secret*) a máte možnost nastavit některé parametry komunikace.

   Poznámka: V případě *Automatické registrace* platnost *Client Secret* za určitou dobu vyprší. Pokud se rozhodnete používat *Automatickou registraci*, je v implementaci potřeba pamatovat na to, aby registraci prodlužovala.

2. Poslat testovací metadata služby (*Client ID*) na podporu (techsupport@mojeid.cz). Podpora nastaví přístupy.
3. *Založit a nastavit testovací účty MojeID* (str. 57).

Implementace a ladění

Budete potřebovat: textový editor, prohlížeč, přístup k hostingu, specifikace OIDC[43]

Pro ladění implementace se vám mohou hodit *naše doporučení k ladícím nástrojům* (str. 48). Během ladění můžete narazit na různá chybová hlášení, při jejichž řešení vám může pomoci *Příloha č. 6 – Příklady a řešení chybových hlášek* (str. 76).

1. *Zavést tlačítko a odkazy MojeID* (str. 38) do (šablon/stránek) služby, přes které bude uživatel žádat o přihlášení. Dodržujte *Zásady správné implementace* (str. 82)!
2. *Získat konfiguraci testovacího poskytovatele OIDC* (str. 38) (webfinger).
3. Konfigurace knihovny – vyplnit testovací *Client ID* a *Client Secret*, případně i testovací endpointy, pokud to knihovna neumí zjistit sama z konfigurace poskytovatele OIDC.
4. *Sestavit a odeslat požadavek na autentizaci* (str. 39) na *Authorization Endpoint* (str. 58).

   Poznámka: Požadavek má mimo jiné obsahovat volbu *schématu autentizace* (str. 8). Kroky popsané dále odpovídají schématu *Přístupový kód*.

[43] https://openid.net/specs/openid-connect-core-1_0.html

5. Zpracovat *odpověď na autentizaci* (str. 41) na návratové adrese uvedené v požadavku, která obdrží *přístupový kód* (`code`).
6. *Sestavit a odeslat požadavek o token* (str. 42) na *Token Endpoint* (str. 58). V požadavku použijete získaný *přístupový kód*.
7. Zpracovat odpověď, z níž získáte *Access Token* (`access_token`) a *ID Token* (`id_token`, Co obsahuje ID Token?[44]), jehož platnost musí implementace ověřit (viz ID Token Validation[45]).
8. Pokud je *ID Token* validní, *sestavit a odeslat požadavek o data uživatele* (str. 43) na *UserInfo Endpoint* (str. 58). V požadavku použijete *Access Token*.
9. Zpracovat odpověď s daty uživatele podle potřeb vaší služby.

Ověření implementace

Pokud budete chtít službu provozovat s plným přístupem, musíme před převedením služby na ostrý provoz provést uživatelské testování vaší implementace.

1. Až dokončíte ladění implementace, zašlete na podporu (techsupport@mojeid.cz) oznámení, že je vaše implementace připravena k uživatelskému testování, a přiložte adresu testovací instance vaší služby.
2. Jakmile společně doladíme poslední detaily, implementace bude připravena pro přechod na ostrý provoz.

[44] https://openid.net/specs/openid-connect-core-1_0.html#CodeIDToken
[45] https://openid.net/specs/openid-connect-core-1_0.html#ImplicitIDTValidation

Přechod na ostrý provoz

1. Pro plný přístup nejprve podepsat smlouvu.
2. *Zaregistrovat službu* (str. 35) (klienta) na *ostrém Registration Endpointu* (str. 58), čímž získáte ostrá metadata svojí služby a nastavíte parametry komunikace.
3. Poslat ostrá metadata služby (*Client ID*) na podporu (techsupport@mojeid.cz) a to i v případě částečného přístupu. Podpora zavede službu do katalogu.
4. *Získat konfiguraci ostrého poskytovatele OIDC* (str. 38) (webfinger).
5. Překonfigurovat implementaci s ostrými metadaty, případně i endpointy.

A je hotovo.

5.1.3 Registrace klienta

Pro komunikaci se službou MojeID přes protokol OpenID Connect je potřeba zaregistrovat klienta (službu) na serveru MojeID. Je možné využít buď ruční, či automatické registrace. *Automatická registrace* (str. 35) je vhodná pro dynamicky vytvářené klienty (JS, mobilní zařízení) a *ruční registrace* (str. 35) je vhodná pro serverové klienty.

Ruční registrace

Ruční registraci lze provést na adrese https://mojeid.cz/consumer_admin/. V případě testovací instance MojeID na adrese https://mojeid.regtest.nic.cz/consumer_admin/. Na stejné adrese lze pak spravované klienty i upravovat či mazat. Takto vytvoření klienti mají dobu platnosti nastavenou na neurčito. Specifikace jednotlivých položek lze nalézt v dokumentaci protokolu OpenID Connect (https://openid.net/specs/openid-connect-registration-1_0.html#ClientMetadata).

Příklad ruční registrace klienta v testovací instanci MojeID:

1. U libovolného účtu, který vytvoříte v *testovací instanci MojeID* (str. 57), přejděte po přihlášení na https://mojeid.regtest.nic.cz/consumer_admin/.
2. Přejděte na odkaz `Založení nové služby`. Vyplňte požadované položky `Název klienta`, `Seznam URI` a klikněte na tlačítko `Uložit`.
   - V seznamu spravovaných služeb se vytvoří záznam s ID klienta.
3. Pro získání `Client secret / Tajemství klienta` přejděte v nově přidané službě na odkaz `Aktualizovat`.
   - Zobrazí se stránka pro editaci nastavení – `Tajemství klienta` najdete v posledním řádku zobrazeného formuláře.

Automatická registrace

Podrobnosti lze nalézt v dokumentaci protokolu OpenID Connect (https://openid.net/specs/openid-connect-registration-1_0.html). O potřebná nastavení by se měla postarat použitá knihovna. Takto vytvořené registrace vyprší po uplynutí 24 hodin, ale je možné je prodlužovat (viz *Změna registrace* (str. 38)).

Pozor: automatickou (dynamickou) registraci nelze využít pro *Plný přístup*.

Příklad registrace klienta s použitím knihovny:

```
from oic.oic.consumer import Consumer

client = Consumer(SessionDB(URL), OIC_CONFIG, client_config=OIC_CLIENT_CONFIG)
client.redirect_uris = URL + client.consumer_config['authz_page']
provider_info = client.provider_config(ISSUER)
client.register(provider_info["registration_endpoint"], response_types='code',␣
↪client_name=MY_CLIENT_NAME)
```

Příklad registračního dotazu:

```
POST /oidc/registration HTTP/1.1
Content-Type: application/json
Accept: application/json
Host: mojeid.cz

{
 "application_type": "web",
 "redirect_uris":
     ["https://client.example.org/callback",
      "https://client.example.org/callback2"],
 "client_name": "My Example",
 "logo_uri": "https://client.example.org/logo.png",
 "token_endpoint_auth_method": "client_secret_post"
}
```

Příklad odpovědi serveru na registrační dotaz:

```
HTTP/1.1 201 Created
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
 "client_id": "s6BhdRkqt3",
 "client_secret": "ZJYCqe3GGRvdrudKyZS0XhGv_Z45DuKhCUk0gBR1vZk",
 "client_secret_expires_at": 1577858400,
 "registration_access_token": "MY.SECRET.REGISTRATION.ACCESS.TOKEN",
 "registration_client_uri": "https://mojeid.cz/oidc/registration?client_
↪id=s6BhdRkqt3",
 "token_endpoint_auth_method": "client_secret_post",
 "application_type": "web",
 "redirect_uris":
     ["https://client.example.org/callback",
      "https://client.example.org/callback2"],
 "client_name": "My Example",
 "logo_uri": "https://client.example.org/logo.png"
}
```

Poznámka: Vyřízení registrace a získání Client ID a Client Secret lze provést i bez knihovny, stačí třeba poslat dotaz POST přes `curl`.

Příklad:

```
curl --data '{"redirect_uris": "https://navratova-adresa.cz",
  "client_name": "Název služby"}' https://mojeid.cz/oidc/registration/
```

Registrace umožňuje také s registrací klienta asociovat metadata (viz Client Metadata ve specifikaci[46]), takže si poskytovatel může nadefinovat např. název a ikonu služby, konkrétně atributy `client_name`, `logo_uri`, případně `client_uri`.

Informace o registraci

Součástí odpovědi serveru MojeID na provedenou registraci je i adresa URL, na které lze získat aktuální informace o registraci (konfigurační endpoint `registration_client_uri`), a přístupový kód (`registration_access_token`). Při dotazu GET na tuto adresu URL je nutné se autentifikovat pomocí přístupového kódu. Ten je nutné zahrnout do hlavičky `Authorization` požadavku HTTP.

Odpověď serveru je ve stejném formátu jako odpověď při registraci a obsahuje aktuální informace o vašem klientovi na našem serveru.

[46] https://openid.net/specs/openid-connect-registration-1_0.html#ClientMetadata

Změna registrace

Pomocí výše uvedeného konfiguračního endpointu je možné i editovat některé informace o registrovaném klientovi. Pro konfiguraci je nutné použít dotaz POST, opět doplněný o `registration_access_token` v hlavičce `Authorization`. Formát požadavku je stejný jako v případě registrace a stejné je i jeho zpracování na serveru s následujícími výjimkami:

- Není možné změnit registrované `redirect_uri` a `client_id`.
- Hodnota `client_secret` je ignorována. V případě přítomnosti položky v dotazu je vygenerován nový `client_secret`. Ten je zaslán v odpovědi na konfigurační dotaz.

Příklad konfiguračního dotazu, který zajistí vygenerování nového `client_secret` a změnu `logo_uri` a `policy_uri`.

```
POST /oidc/registration?client_id=MYCLIENTID HTTP/1.1
Accept: application/json
Host: mojeid.cz
Authorization: Bearer MY.SECRET.REGISTRATION.ACCESS.TOKEN

{
 "client_secret": null,
 "logo_uri": "https://client.example.org/another-logo.png",
 "policy_uri": "https://client.example.org/policy-page"
}
```

Odpověď serveru na konfigurační dotaz je stejná jako odpověď na registrační dotaz a obsahuje aktuální informace o vašem klientovi na našem serveru.

5.1.4 Žádost o přihlášení přes MojeID

Proces ověřování uživatelovy identity začne tím, že na vašich stránkách uživatel podá žádost o přihlášení přes MojeID. Pro maximální uživatelskou přívětivost stačí pouze tlačítko pro přihlášení „Přihlásit přes MojeID“, viz soubor *Grafické prvky* na stránce Jak zavést[47]. Uživatelské jméno uživatel zadá později na serveru MojeID.

Přihlašování ke službě MojeID tlačítkem je jediná doporučená a správná metoda.

5.1.5 Iniciace

Abyste mohli odeslat žádost o ověření identity, potřebuje vaše knihovna znát buď identifikátor uživatele nebo koncový bod OCP.

Pomocí identifikátoru nebo koncového bodu provede vaše aplikace WebFinger dotaz pro zjištění podrobností o OpenID Connect poskytovateli. Odpověď na tento dotaz obsahuje mimo jiné i:

- **Autorizační endpoint** – to je vždy `https://mojeid.cz/oidc/authorization/` a na tuto adresu budou směřovány žádosti o ověření identity.
- **Token endpoint** – to je vždy `https://mojeid.cz/oidc/token/` a na tuto adresu jsou směřovány žádosti o token.

[47] https://www.mojeid.cz/cs/pro-poskytovatele/jak-zavest/

- **UserInfo endpoint** – to je vždy `https://mojeid.cz/oidc/userinfo/` a na tuto adresu jsou směřovány žádosti o uživatelská data.

Příklad dotazu na konkrétního uživatele:

```
GET /oidc/.well-known/webfinger?resource=acct%3Ajoe%40mojeid.cz&rel=http%3A%2F
↪%2Fopenid.net%2Fspecs%2Fconnect%2F1.0%2Fissuer HTTP/1.1
Host: mojeid.cz
```

Příklad odpovědi serveru:

```
HTTP/1.1 200 OK
Content-Type: application/jrd+json

{
 "subject": "acct:joe@mojeid.cz",
 "links": [
    {"rel": "http://openid.net/specs/connect/1.0/issuer",
     "href": "https://mojeid.cz/oidc/"}
 ]
}
```

5.1.6 Žádost o ověření identity

Jakmile znáte koncový bod OCP, zašle vaše aplikace skrze přesměrování uživatelova prohlížeče žádost o ověření identity (autentizaci). Žádost obsahuje speciální parametry pro její realizaci. O správné uvedení těchto parametrů se opět postará použitá OpenID Connect knihovna použitá pro implementaci.

Žádost o ověření identity obsahuje obvykle následující parametry:

- **Návratovou adresu (URL) aplikace** – Na tuto adresu se vrátí uživatel po přihlášení ze stránek poskytovatele OpenID Connect a zde bude výsledek přihlášení zpracován.
- **Požadované skupiny údajů z MojeID** – Žádost o ověření identity musí jako požadovanou skupinu údajů obsahovat alespoň *openid*.
- **Požadované údaje z MojeID** – Do žádosti o ověření identity lze přidat i seznam jednotlivých údajů z MojeID identity, které vaše aplikace vyžaduje a které budou po úspěšném přihlášení a se souhlasem uživatele aplikaci předány. Pro každý údaj je nutné uvést jeho identifikátor. Údaje a jejich identifikátory obsahuje *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62). Tento seznam je ve formátu JSON specifikovaném v dokumentaci OpenID Connect[48]. Položky mohou být označeny za povinné pomocí výrazu `"essential": true`.

Příklad položek v požadavku, které může žádost o ověření identity obsahovat, shrnuje následující tabulka:

[48] https://openid.net/specs/openid-connect-core-1_0.html#ClaimsParameter

Parametr (klíč)	Popis a hodnota
`scope`	Seznam požadovaných skupin údajů *openid address*
`response_type`	Určení požadovaného schématu autentizace *id_token*
`client_id`	Jednoznačný identifikátor poskytovatele služeb *test_clienti*
`redirect_uri`	Návratová adresa z MojeID. *http://www.poskytovatel-example.cz/*

`claims`	Podrobnější specifikace požadovaných údajů.
	`{"userinfo":`
	`{"name": null,`
	`"nickname": {"essential": true}}`
	`}`

Příklad požadavku na autentizaci:

```
sid, location = client.begin(path=URL, scope=SCOPE)
HttpResponseRedirect(location)
```

Příklad dotazu požadavku na autentizaci:

Výpis 1: Příklad vyžádání údajů pomocí „scope“ (skupiny údajů)

```
GET /oidc/authorization/?response_type=code&scope=openid%20profile%20email&
↪client_id=s6BhdRkqt3&state=af0ifjsldkj&redirect_uri=https%3A%2F%2Fclient.
↪example.org%2Fcb HTTP/1.1
Host: mojeid.cz
```

Výpis 2: Příklad vyžádání údajů pomocí „claims“ (jednotlivé údaje)

```
GET /oidc/authorization/?state=950ba54cb302a7c6a814f22a4e5c5445&redirect_
↪uri=https%3A%2F%2Fmojeid.cz%3A8000%2Fconsumer%2Foic%2Ffinish%2F&response_
↪type=code&client_id=8ol68PATaSpA&scope=openid&claims=%7B%22userinfo%22%3A+%7B
↪%22name%22%3A+null%2C+%22nickname%22%3A+%7B%22essential%22%3A+true%7D%7D%7D&
↪ui_locales=off HTTP/1.1
Host: mojeid.cz
```

Odpověď od serveru přijde až po kroku provedení autentizace. Příklad odpovědi je uveden v sekci *Odpověď na autentizaci* (str. 41).

5.1.7 Provedení autentizace

V okamžiku, kdy uživatel dorazí s žádostí o ověření identity na server MojeID, je mu zobrazena přihlašovací stránka, kde proběhne samotné přihlášení.

Obr. 1: *Přihlašovací stránka MojeID*

Tato autentizace je provedena servery MojeID. V rámci tohoto ověření se pokusíme provést maximum úkonů, které byly specifikovány pomocí parametrů v žádosti o ověření identity. Celý proces se odehrává pouze v systémech MojeID a z vaší strany nevyžaduje žádnou činnost.

5.1.8 Odpověď na autentizaci

Poté, co uživatel dokončí proces autentizace, obdržíte ze serverů MojeID odpověď s jejím výsledkem. Struktura a obsah této odpovědi se liší v závislosti na vybraném komunikačním schématu (viz *Proces komunikace přes OpenID Connect* (str. 8)).

V případě využití komunikace přes *Implicitní schéma* (str. 9) je v odpovědi obsažen identifikátor uživatele a ID token, který může obsahovat data o uživateli.

V případě použití komunikace přes *Přístupový kód* (str. 10) nebo *Hybridní schéma* (str. 11) obsahuje odpověď přístupový kód (access code), který je nutné použít v dalším kroku autentifikačního procesu.

Příklad zpracování odpovědi:

```
aresp, _, _ = client.parse_authz(request.GET.urlencode())
```

Příklad odpovědi serveru:

```
HTTP/1.1 302 Found
Location: https://client.example.org/cb?code=SplxlOBeZQQYbYS6WxSbIA&
↪state=af0ifjsldkj
```

5.1.9 Žádost o token

Pokud jste v předchozím kroku autentizace obdrželi přístupový kód (access code), musíte ho na Token endpointu vyměnit za platný token.

V případě použití komunikace přes *Hybridní schéma* (str. 11) obsahuje odpověď přístupový token a ID token, který může obsahovat data o uživateli. V tomto případě je proces autentizace a předání údajů dokončen.

Při komunikaci přes *Přístupový kód* (str. 10) je v odpovědi opět obsažen token a ID token, ale ten neobsahuje data o uživateli. O ta je nutné si zažádat v dalším kroku.

Příklad komunikace:

```
POST /oidc/token/ HTTP/1.1
Host: mojeid.cz
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA&redirect_uri=https%3A
↪%2F%2Fclient.example.org%2Fcb
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
 "access_token": "SlAV32hkKG",
 "token_type": "Bearer",
 "refresh_token": "8xLOxBtZp8",
 "expires_in": 3600,
 "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzc
              yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5
              NzYxMDAxIiwKICJhdWQiOiAiczZCaGRSa3F0MyIsCiAibm9uY2UiOiAibiOwUzZ
              fV3pBMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5Nz
              AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzROEHR9R6jgdqrOOF4daGU96Sr_P6q
              Jp6IcmD3HP99Obi1PRs-cwh3LO-p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJ
              NqeGpe-gccMg4vfKjkM8FcGvnzZUN4_KSP0aAp1tOJ1zZwgjxqGByKHiOtX7Tpd
              QyHE5lcMiKPXfEIQILVq0pc_E2DzL7emopWoaoZTF_m0_N0YzFC6g6EJbOEoRoS
              K5hoDalrcvRYLSrQAZZKflyuVCyixEoV9GfNQC3_osjzw2PAithfubEEBLuVVk4
              XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg"
}
```

5.1.10 Žádost o data

V tomto kroku použijete token získaný v předchozím kroku autentizace k získání dat o uživateli. Data je nutné vyzvednout na UserInfo endpointu.

UserInfo endpoint vždy vrací v odpovědi atribut `sub` (*subject*), který jednoznačně identifikuje uživatele a měl by být použit k validaci odpovědi podle *ID Token*.

Data o uživateli by měla být dále zpracována jen v případě, že odpověď byla shledána validní.

Příklad žádosti o data:

```
state = aresp.to_dict()['state']
resp = client.complete(state)
uinfo = client.get_user_info(state)
```

Příklad komunikace se serverem:

```
GET /oidc/userinfo/ HTTP/1.1
Host: mojeid.cz
Authorization: Bearer S1AV32hkKG
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{
 "sub": "248289761001",
 "name": "Jane Doe",
 "given_name": "Jane",
 "family_name": "Doe",
 "preferred_username": "j.doe",
 "email": "janedoe@example.com"
}
```

5.1.11 Knihovna MojeID LITE

Javascriptová knihovna **MojeID LITE** (nebo také MojeID Connect) umožňuje načtení údajů z identity MojeID do webové stránky na straně klienta za využití protokolu OpenID Connect.

Tuto funkcionalitu je možné využít například pro jednoduché předvyplnění webového formuláře údaji uživatele, který má aktivní účet MojeID.

Abyste existující formulář rozšířili o tuto funkcionalitu, musíte provést minimálně následující kroky:

1. *Vložit odkaz na knihovnu.*

   Tuto knihovnu je možné vystavit na vlastním serveru, pokud chcete snížit závislost na externím webu. Knihovna je ke stažení na této adrese[49]. Knihovna závisí na kryptografické knihovně jsrsasign[50], která je v aktuální verzi k dispozici i na našem webu, takže není nutné ji vkládat přímo. Kód skriptu pro vložení knihovny musí být v sekci `<HEAD>`.

   Příklad vložení knihovny:

   ```
   <script type="text/javascript"
      src="https://www.mojeid.cz/public/media/1542958574/150/"
      data-jsrsasign="https://www.mojeid.cz/public/media/1542956522/149/">
   </script>
   ```

2. *Zavolat funkci na vytvoření objektu MojeidConnect.*

   Tento objekt reprezentuje komunikaci se serverem MojeID. Při volání vytvářející funkce je možné *nastavit některé parametry* (str. 45), které ovlivní proces předání údajů. Kód skriptu s voláním funkce musí být v sekci `<HEAD>`.

   Příklad vytvoření objektu:

   ```
   <script type="text/javascript"> (function() {
      mojeid = createMojeidConnect( {
         clientName: "Ukázkový formulář",
         claims: ['phone_number', 'family_name', 'given_name', 'nickname',
            'email', 'address', 'birthdate', 'gender', 'website', 'profile']
      } );
   })();</script>
   ```

3. *Na tlačítko, které aktivuje předvyplnění formuláře, navěsit volání metody requestAuthentication().*

   Tato metoda zajistí nastartování autentizačního procesu a vyplnění hodnot odsouhlasených údajů do formuláře.

   Příklad kódu pro tlačítko:

   ```
   <button onclick="mojeid.requestAuthentication()">
   Předvyplnit pomocí MojeID
   </button>
   ```

[49] https://www.mojeid.cz/public/media/1542958574/150/
[50] https://kjur.github.io/jsrsasign/

Parametry funkce createMojeidConnect(options)

Při volání této funkce je možné ve slovníkové struktuře určit některé parametry, které ovlivní komunikaci se serverem MojeID:

`clientId`

Je možné, že je služba již zaregistrovaná v MojeID serveru. Pokud ano má tato služba přidělené clientId a toto je možné uvést v parametru. Pokud není clientId vyplněné, dojde k dynamické registraci podle specifikace OpenID Connect[51] s využitím adresy uvedené v parametru `regEndpoint`. **Pozor:** automatickou (dynamickou) registraci nelze využít pro *Plný přístup*.

`clientName`

V případě dynamické registrace je možné zde uvést název služby, který se zobrazí uživateli při schválení předání údajů. Pokud nebude název uveden, použije se URL služby.

`scope`

Požadované předávané údaje v podobě skupin údajů. Hodnotou je podseznam `['openid', 'profile', 'email', 'phone', 'address']`, přičemž `'openid'` musí být uveden vždy. Pokud není uveden, je hodnota `['openid']`.

`claims`

Požadované předávané údaje v podobě jednotlivých atributů. Hodnotou je seznam atributů. Úplný seznam možných atributů je k dispozici v hodnotě `claims_supported` z konfiguračního souboru serveru[52]. Jako příklad může sloužit tento seznam: `['phone_number', 'family_name', 'given_name', 'nickname', 'email', 'address', 'birthdate', 'gender', 'website', 'profile']`

`attrDict`

Knihovna předpokládá, že položky formuláře mají stejné `id` jako je název atributu ze seznamu `claims`. Pokud toto není pravda, je v tomto parametru možné uvést mapovací seznam pro id formulářové položky a název atributu.

`formCallback`

Pokud nestačí mapovací slovník z `attrDict`, je zde možné uvést název vlastní JS funkce, která se postará o vyplnění formuláře.

`display`

Hodnota je buď `popup` nebo `redirect` podle toho, zda se přihlášení má provést v novém okně nebo ve stávajícím. Výchozí hodnota je `popup`.

`regEndpoint`

URL registračního endpointu podle specifikace protokolu OpenID Connect[53]. Výchozí hodnota je `https://mojeid.cz/oidc/registration/`.

`authEndpoint`

[51] https://openid.net/specs/openid-connect-registration-1_0.html
[52] https://mojeid.cz/oidc/.well-known/openid-configuration/
[53] https://openid.net/specs/openid-connect-registration-1_0.html

URL autentizačního endpointu podle specifikace protokolu OpenID Connect[54]. Výchozí hodnota je `https://mojeid.cz/oidc/authorization/`.

Ukázkový formulář

Pro snazší porozumění si můžete on-line prohlédnout a vyzkoušet kompletní ukázkový formulář[55].

5.1.12 Žádost o ověření identity účtem napojeným na NIA

Žádost o ověření identity účtem MojeID napojeným na NIA se vyžádá pomocí parametru `acr_values`. Hodnoty pro vyžádání konkrétní úrovně záruky shrnuje tabulka níže.

ACR value	Popis
`http://eidas.europa.eu/LoA/substantial`	eIDAS úroveň záruky „značná“
`http://eidas.europa.eu/LoA/high`	eIDAS úroveň záruky „vysoká“

Detailní informace o `acr_values` lze nalézt přímo v dokumentaci OpenID Connect na následujících odkazech:

- ID Token[56].
- Authentication Request[57].
- Requesting the „acr“ Claim[58].

[54] https://openid.net/specs/openid-connect-registration-1_0.html
[55] https://www.mojeid.cz/public/media/1542960671/153/
[56] https://openid.net/specs/openid-connect-core-1_0.html#IDToken
[57] https://openid.net/specs/openid-connect-core-1_0.html#AuthRequest
[58] https://openid.net/specs/openid-connect-core-1_0.html#acrSemantics

5.2 Implementace pomocí SAML

SAML je protokol, který historicky předchází moderním protokolům OpenID. Pokud váš systém již podporuje SAML (například se jedná o instalaci systému Shibboleth nebo podobných) je možné využít pro napojení na MojeID i tohoto protokolu.

Implementace protokolu SAML 2.0 vychází ze specifikací na https://wiki.oasis-open.org/security/FrontPage

Pro napojení na MojeID je nutné zaslat metadata služby na adresu techsupport@mojeid.cz a případně zaregistrovat metadata MojeID, která jsou uvedena na https://mojeid.cz/saml/idp.xml. Certifikát uvedený v metadatech se může změnit a proto je potřeba čas od času tato metadata aktualizovat. Pro ověření podpisu metadat je možné použít certifikát na https://mojeid.cz/saml/cert.

Jelikož jsou SAML zprávy *base64-encoded* a *deflated*, můžete si je za účelem odlaďování převést do čitelného XML např. pomocí nástroje https://www.samltool.com/decode.php.

Seznam údajů, které mohou být protokolem předány, (vč. jejich identifikátorů) obsahuje *Příloha č. 3 – Seznam údajů pro předání (SAML)* (str. 67) a *Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69).

Příklady a řešení chybových hlášek obsahuje *Příloha č. 6 – Příklady a řešení chybových hlášek* (str. 76).

5.2.1 Žádost o ověření identity účtem napojeným na NIA

Žádost o ověření identity účtem MojeID napojeným na NIA se vyžádá pomocí třídy `AuthnContextClassRef` (Authentication Context Class Reference). Hodnoty pro vyžádání konkrétní úrovně záruky shrnuje tabulka níže.

AuthnContextClassRef	Popis
`http://eidas.europa.eu/LoA/substantial`	eIDAS úroveň záruky „značná“
`http://eidas.europa.eu/LoA/high`	eIDAS úroveň záruky „vysoká“

Příklad použití:

```
<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    http://eidas.europa.eu/LoA/substantial
</saml:AuthnContextClassRef>
```

5.3 Problémy při implementaci

Tato sekce upozorňuje na některé problémy při implementování a naznačuje jejich řešení nebo obejití.

5.3.1 Rozdíly mezi protokoly

Závažným rozdílem mezi protokoly je, že každý protokol je schopný předat jen některé údaje z identity MojeID a tato množina údajů je u každého protokolu jiná.

Pracujeme na jejich sjednocení, ale v současnosti **není možné** předat všechny údaje identity přes každý z podporovaných protokolů.

Předávané údaje jsou vypsány pro jednotlivé protokoly v přílohách:

- *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62)
- *Příloha č. 3 – Seznam údajů pro předání (SAML)* (str. 67) a
- *Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69)

5.3.2 Přechod na jiný protokol

Obecně probíhá přechod na jiný protokol tak, že se uživatel přes nějakou ze stávajících přihlašovacích metod přihlásí do služby a poté se přihlásí znovu pomocí nového protokolu. Tím může poskytovatel služby přiřadit existujícímu uživateli identifikátor nového protokolu.

Přechod z protokolu OpenID 2.0 na nový protokol OpenID Connect

Chcete-li přejít z původního protokolu OpenID 2.0 na aktuální protokol OpenID Connect, odešlete žádost o ověření identity protokolem OpenID Connect s parametrem `scope` rozšířeným o hodnotu `openid2` a zpět obdržíte identitu OpenID 2.0 spolu s identitou OpenID Connect.

Více informací o procesu migrace najdete v těchto specifikacích[59].

5.3.3 Ladění komunikace se serverem MojeID

Pro ladění problémů v komunikaci doporučujeme použít vývojářské nástroje ve webovém prohlížeči. Ty umožňují prohlížet síťové aktivity, tedy dotazy a odpovědi zasílané mezi klientem (vaše implementace) a serverem MojeID. To vám může pomoct odhalit případnou chybu v předávaných datech.

Poznámka: U složitějších problémů, kdy se musíte obrátit na naši technickou podporu, je užitečné pro analýzu problému přidat k popisu i zachycený výpis komunikace.

Ve `Firefoxu` je možné použít vestavěné nástroje nebo doplněk (např. FireBug):

1. Nástroje pro vývojáře zapnete přes *hlavní menu* → *Vývojář* nebo klávesovou zkratkou `Ctrl+Shift+I`.
2. Poté přepněte na záložku *Síť* (nebo vyvolejte přímo záložku klávesovou zkratkou `Ctrl+Shift+Q`).

V `Chrome` je též možné použít vestavěné nástroje:

1. Nástroje pro vývojáře zapnete přes *hlavní menu* → *Další nástroje* → *Nástroje pro vývojáře* nebo klávesovou zkratkou `Ctrl+Shift+I`.
2. Poté přepněte na záložku *Network*.

[59] https://openid.net/specs/openid-connect-migration-1_0.html

Odlaďování v popup okně

Pokud ověření uživatele přes MojeID implementujete pomocí nového popup okna, je pro odchyt komunikace potřeba:

1. Poprvé nechat vygenerovat popup okno.
2. Před odesláním požadavku na server MojeID v něm kliknout pravým tlačítkem myši a otevřít ladicí nástroj výběrem položky v nabídce:
   - Chromium: *Prozkoumat*
   - Firefox: *Prozkoumat prvek*
   - FireBug plugin: *Prozkoumat prvek ve firebug*
3. Vyvolat obnovení popup okna (např. `F5` nebo `Ctrl+R`).
4. Standardně pokračovat v odchytu síťové komunikace v ladicím nástroji.

Kapitola 6

Rozhraní pro zakládání účtů MojeID

Tato kapitola popisuje mechanismus registrace účtů MojeID prostřednictvím vaší aplikace.

6.1 Žádost o založení účtu MojeID

Uživatel si ve vaší aplikaci zvolí možnost založit účet MojeID. Toto vygeneruje v prohlížeči uživatele HTTPS POST požadavek na registrační server na adrese `https://direct.mojeid.cz/registration/direct/`. V parametrech požadavku jsou spolu s požadovaným uživatelským jménem všechny evidované údaje o daném uživateli (Seznam údajů pro registraci obsahuje *Příloha č. 5 – Seznam údajů pro registraci* (str. 72)) a navíc:

- **identifikátor poskytovatele služeb** (`realm`) – volitelné URI, jehož hodnota závisí na komunikačním protokolu:
  - v případě OpenID Connect se musí jednat o přidělené `client_id`,
- **jednoznačný identifikátor transakce** (`registration_nonce`) – slouží ke spárování odpovědi na tento požadavek.

Také máte možnost volbou adresy `https://mojeid.cz/transfer/endpoint/` nabídnout uživateli převod existujícího kontaktu v centrálním registru. V takovém případě se ignorují zaslané údaje o uživateli a je vyplněno uživatelské jméno, neboli identifikátor kontaktu, který nelze měnit. Pokud je identifikátor nevalidní, nelze ho převést do MojeID, uživatel musí kontaktovat určeného registrátora pro změnu.

Dále je uživateli zobrazen formulář se seznamem údajů, které se po registraci vloží do MojeID. U základních údajů se zobrazí i hodnota a je možné je změnit. Uživatel na registračním formuláři následně:

- odsouhlasí pravidla používání služby,
- bude ověřen pomocí CAPTCHA.

6.2 Kontrola validity dat

Registrační server po odeslání formuláře zkontroluje validitu dat a nechá uživatele opravit chyby. V případě, že jsou data validní, je zahájen proces registrace nového účtu. Do tohoto účtu registrační server uloží požadovaná data a připojí vaši identifikaci (identifikátor poskytovatele služeb, realm). Následně je zahájena identifikace uživatele zadáním ověřovacích kódů zaslaných na e-mail a telefonní číslo.

Následujícím krokem je informovat vaši aplikaci o úspěšné registraci.

V případě komunikace přes OpenID Connect musí být URL pro zasílání informací zadány v průběhu *registrace klienta* (str. 35) pomocí `assertion_uris` klíče, do kterého se vkládá seznam adres (zakódovaný do JSON), na které se mají zprávy odesílat.

Vaší aplikaci je přímo poslána HTTPS POST zpráva na rozhraní dané adresou URL. Obsahem zprávy jsou tři parametry:

- `registration_nonce` – jednoznačný identifikátor transakce pro spárování s původním požadavkem,
- identifikátor uživatele MojeID:
  - `sub` – v případě protokolu OpenID Connect,
- `status` – stav s hodnotou `REGISTERED`.

Vaše aplikace musí tuto zprávu nejprve ověřit:

- Musí zkontrolovat, že zpráva byla doručena na některou z adres uvedených v bodě *Žádost o založení účtu MojeID* (str. 51).
- Musí ověřit, že transakce `registration_nonce` byla opravdu vytvořena.
- Musí ověřit, že klientský certifikát, použitý pro vytvoření SSL tunelu, je platný a podepsaný certifikační autoritou CZ.NIC. Pokud takový certifikát nemáte, zašlete nám prosím identifikátor poskytovatele služeb (clientID) na techsupport@mojeid.cz. Certifikát u nás vytvoříme a zašleme.

Pokud nepoužíváte HTTPS a chcete na testovacím prostředí zkoušet přihlašování a zakládání účtů, tento certifikát není třeba.

Pokud HTTPS používáte a jde o testovací prostředí, je tento certifikát potřeba pro zasílání notifikací z registrace. Pro přihlášení není třeba (mezi MojeID a vaším serverem se přenáší jen obecná veřejná data, takže není třeba ověřovat „totožnost“ toho, kdo je žádá).

Notifikace se posílají po registraci, částečné identifikaci (ověření e-mailu a telefonu) a identifikaci (zadán PIN3, pouze do roku 2024) na `assert_url`, které je uvedeno v XRDS dokumentu na realmu. Toto je funkční i na testu. Aby vaše aplikace dostávala notifikace, musíte mít realm s HTTPS. Dále pak po přijetí notifikace je třeba odpovědět řetězcem `'mode:accept\n'`, kde `\n` je znak nové řádky.

Tip: Ověřování klientského certifikátu umí zajistit HTTP server např. Apache s použitím konfigurační volby `SSLVerifyClient`.

Pokud jsou všechny podmínky splněny, může vaše aplikace při zpracování této zprávy spárovat MojeID identifikátor se svým záznamem o uživateli pro účely autentizace přes MojeID.

Poznámka: Pokud není možné zaslat tuto zprávu bezpečným způsobem protokolem HTTPS, pokračuje registrace bez zaslání této zprávy.

6.3 Dokončení registrace

Vaše aplikace odešle odpověď na zprávu z bodu *Kontrola validity dat* (str. 51) v těle HTTP odpovědi ve formátu klíč-hodnota OpenID protokolu:

- **výsledek** (`mode`) – hodnota `accept` nebo `reject` značící, zda uživatelův účet byl úspěšně spárován,
- **důvod zamítnutí** (`reason`) – nepovinný parametr obsahující důvod, proč k párování nedošlo.

Pokud nebude obdržena odpověď ve správném formátu, bude zpráva s výsledkem registrace poslána na další adresu z bodu *Kontrola validity dat* (str. 51), dokud nebude získána odpověď nebo nebudou adresy vyčerpány.

Registrace pak pokračuje buď přímou výzvou k ověření e-mailové adresy a telefonního čísla a vstoupením do profilu, kde si uživatel zvolí heslo, nebo je uživateli zobrazena informace o dokončení registrace.

Pokud máte aktivován *plný přístup*, budou vaší aplikaci zasílány informace i o změně stavu uživatelova účtu. Tyto zprávy jsou posílány podobně jako v bodě *Kontrola validity dat* (str. 51), se dvěma parametry v každé zprávě:

- **identifikátor uživatele MojeID:**
  - `sub` – v případě OpenID Connect.
- `status` **– stav účtu, jedna z hodnot:**
  - `CONDITIONALLY_IDENTIFIED` **– částečně identifikovaný.**
    - Účet s ověřeným e-mailem a telefonním číslem.
    - U účtů do roku 2024 zadán PIN1 a PIN2.
  - `IDENTIFIED` **– identifikovaný (zadán PIN1, PIN2 a PIN3**[Strana 53, 60]**).**
    - Pouze u účtů do roku 2024.
  - `VALIDATED` **– validovaný (účet s příznakem validace).**
    - Validovaný účet právnické osoby nebo účet fyzické osoby napojený na systémy veřejné správy (NIA).
    - U účtů do roku 2024 zadán PIN1, PIN2, PIN3[61] a příznak validace.

Pokud selže odesílání této zprávy nebo na ni nebude správně odpovězeno, bude informace o změně stavu zaslána opakovaně každých 5 minut po dobu 6 hodin, dokud je vaše aplikace nepřijme nebo neodmítne. Oproti tomu zpráva o dokončení registrace je synchronní – posílá se jen jednou.

Od července 2022 nelze ověřit účty fyzických osob pomocí PIN3. Ověření pomocí PIN3 je možné pouze u účtů s vyplněným polem Organizace.

[60] PIN3 pro identifikaci účtu MojeID není povinný. Identifikaci lze získat napojením účtu na NIA či validací. Může tedy nastat situace, kdy uživatel má identifikovaný účet, ale má zadaný jen PIN1 a PIN2.

[61] PIN3 pro validaci účtu MojeID není povinný. Může tedy nastat situace, kdy uživatel má validovaný účet, ale má zadaný jen PIN1 a PIN2.

Důležité: Od roku 2024 se PIN1, PIN2 a PIN3 pro ověření nepoužívají.

Kapitola 7

Odhlašování od služby MojeID

Z principu fungování MojeID vaše služba uživatele odhlásit z MojeID automaticky nemůže, protože by ho tak odhlásila i od dalších služeb, ke kterým je uživatel přihlášen přes MojeID. Ve výjimečných případech ale může uživatel potřebovat i odhlášení z MojeID, například pokud se přihlásil z cizího zařízení.

Pak je vhodné, aby při nebo po odhlášení z vaší služby, byla uživateli nabídnuta možnost odhlášení i ze služby MojeID.

Pokud uživatel tuto možnost zvolí, uživatele přesměrujte nebo odkažte na adresu `https://mojeid.cz/logout/`, kde uživatel odhlášení potvrdí.

Doporučujeme tuto možnost zavést, pokud se k vaší službě přistupuje z veřejných počítačů (např. v knihovně nebo internetové kavárně) a zároveň to není bezpečně řešeno např. smazáním dat po ukončení práce s prohlížečem.

Jinak ale její zavedení není povinné.

Kapitola 8

Testovací instance MojeID

Pro účely testování implementace můžete využít naši testovací instanci služby MojeID, na níž můžete testovat přihlášení uživatelů MojeID, registrace nových účtů a převody účtů z centrálního registru.

Před zahájením testování zašlete na adresu techsupport@mojeid.cz metadata, pod kterými budete testovat. Tato metadata jsou pro každý protokol jiná, viz informace k jednotlivým protokolům níže.

Důležité: Použijte jiná metadata než pro ostrý provoz!

My vám na testovacím serveru povolíme přístupy a nastavíme pro účely testování tzv. *plný přístup*, aby vám mohly být předávány všechny údaje účtu MojeID, včetně údajů `status`, `valid` a dalších, které jsou předávány pouze poskytovatelům s *plným přístupem*.

8.1 Testovací účty

Pro testování MojeID doporučujeme založit 3 testovací uživatele v různých stupních ověření. K založení účtů využijte návod na úvodní stránce veřejné testovací instance MojeID[62]. Kontaktní a osobní údaje můžete vyplnit libovolné.

- **Částečně identifikovaný účet:**
  - Účet s ověřeným e-mailem a telefonním číslem.
- **Účet fyzické osoby napojený na služby veřejné správy:**
  - Pro napojení testovacího účtu na služby veřejné správy budete potřebovat certifikovaný fyzický nebo systémový bezpečnostní klíč.
  - Založte účet fyzické osoby.
  - Klikněte na `Ověřit totožnost`, poté na `Ověřit se jinak` a vyberte `Testovací profily (LoA High jako eObčanka)`.
  - Zvolte si libovolný testovací profil a dokončete ověření.
- **Účet právnické osoby s validací:**
  - Založte účet právnické osoby.
  - Přejděte do záložky s osobními údaji a klikněte na tlačítko `Validovat`.
  - Stáhněte vygenerovaný PDF dokument a zašlete ho na adresu techsupport@mojeid.cz.
  - Účtu nastavíme příznak validace.

Tím je možné otestovat vracené hodnoty v parametru `status` pro všechny současné varianty ověření účtu.

[62] https://mojeid.regtest.nic.cz/index.html

8.2 Společné endpointy

Část adres rozhraní je nezávislá na vybraném protokolu. Tyto adresy jsou vyjmenovány zde. Dále však budete potřebovat ještě adresy endpointů specifických pro jednotlivé protokoly, které jsou uvedeny níže.

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

- Registrace nového účtu MojeID: `https://mojeid.regtest.nic.cz/registration/endpoint/`
- Převod kontaktu do MojeID z registru domén: `https://mojeid.regtest.nic.cz/transfer/endpoint/`

Pro zavedení implementace MojeID na ostrý provoz budou k dispozici následující adresy:

- Registrace nového účtu MojeID: `https://mojeid.cz/registration/endpoint/`
- Převod kontaktu do MojeID z registru domén: `https://mojeid.cz/transfer/endpoint/`

8.3 OpenID Connect

Potřebná metadata k zaslání na podporu

- `Client_ID`, pod kterým budete testovat – kombinace 12 znaků malých a velkých písmen abecedy a číslic, která je vygenerována automaticky při registraci služby

Endpointy specifické pro protokol

- **Adresy testovacích endpointů:**
  - Registration Endpoint: `https://mojeid.regtest.nic.cz/oidc/registration/`
  - Authorization Endpoint: `https://mojeid.regtest.nic.cz/oidc/authorization/`
  - Token Endpoint: `https://mojeid.regtest.nic.cz/oidc/token/`
  - UserInfo Endpoint: `https://mojeid.regtest.nic.cz/oidc/userinfo/`

  Kompletní popis konfigurace OIDC ve formátu JSON: https://mojeid.regtest.nic.cz/.well-known/openid-configuration/
- **Adresy ostrých endpointů:**
  - Registration Endpoint: `https://mojeid.cz/oidc/registration/`
  - Authorization Endpoint: `https://mojeid.cz/oidc/authorization/`
  - Token Endpoint: `https://mojeid.cz/oidc/token/`
  - UserInfo Endpoint: `https://mojeid.cz/oidc/userinfo/`

  Kompletní popis konfigurace OIDC ve formátu JSON: https://mojeid.cz/.well-known/openid-configuration/

8.4 SAML

Metadata testovací instance jsou na adrese: https://mojeid.regtest.nic.cz/saml/idp.xml

Potřebná metadata k zaslání na podporu

- řetězec `entityID`, pod kterým budete testovat – maximální délka 1024 znaků, specifikace doporučuje, aby řetězec měl podobu adresy URL[63] a obsahoval doménové jméno poskytovatele nebo poskytované služby

  Příklad: `https://sluzba.example.cz`

- soubor XML s metadaty služby (`EntityDescriptor`), který obsahuje totéž `entityID`

  Získat soubor s metadaty vám může pomoci tento článek o přípravě metadat[64].

Endpointy specifické pro protokol

- testovací koncový bod: `https://mojeid.regtest.nic.cz/saml/`
- ostrý koncový bod: `https://mojeid.cz/saml/`

[63] https://en.wikipedia.org/wiki/URL#Syntax
[64] https://www.eduid.cz/cs/tech/metadata-preparation

Kapitola 9

Přílohy

Seznam příloh

9.1 Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)

Údaj	Indentifikátor *claim*u	Datový typ
OpenID2 identifikátor pro migraci ze staršího protokolu	openid2_id	*SINGLE_OPTIONAL_STRING*
Jméno		
Celé jméno	name	*SINGLE_OPTIONAL_STRING*
Křestní jméno	given_name	*SINGLE_OPTIONAL_STRING*
Příjmení	family_name	*SINGLE_OPTIONAL_STRING*
Přezdívka	nickname	*SINGLE_OPTIONAL_STRING*
E-mail		
Hlavní	email	*SINGLE_OPTIONAL_STRING*
Příznak – E-mail ověřen	email_verified	*SINGLE_OPTIONAL_BOOLEAN*
Notifikační	mojeid_email_notify	*SINGLE_OPTIONAL_STRING*
Další	mojeid_email_next	*SINGLE_OPTIONAL_STRING*
Adresa trvalého bydliště / sídla firmy		
Kompletní adresa	mojeid_address_def	*OPTIONAL_ADDRESS_STRING*
Ulice	mojeid_address_def_street	*SINGLE_OPTIONAL_STRING*
Ulice 2	mojeid_address_def_street2	*SINGLE_OPTIONAL_STRING*
Ulice 3	mojeid_address_def_street3	*SINGLE_OPTIONAL_STRING*
Město	mojeid_address_def_city	*SINGLE_OPTIONAL_STRING*
Stát	mojeid_address_def_state	*SINGLE_OPTIONAL_STRING*
PSČ	mojeid_address_def_postal_code	*SINGLE_OPTIONAL_STRING*
Země	mojeid_address_def_country	*SINGLE_OPTIONAL_STRING*
Korespondenční adresa		
Kompletní adresa	address	*OPTIONAL_ADDRESS*
Ulice	mojeid_address_mail_street	*SINGLE_OPTIONAL_STRING*
Ulice 2	mojeid_address_mail_street2	*SINGLE_OPTIONAL_STRING*
Ulice 3	mojeid_address_mail_street3	*SINGLE_OPTIONAL_STRING*
Město	mojeid_address_mail_city	*SINGLE_OPTIONAL_STRING*
Stát	mojeid_address_mail_state	*SINGLE_OPTIONAL_STRING*
PSČ	mojeid_address_mail_postal_code	*SINGLE_OPTIONAL_STRING*
Země	mojeid_address_mail_country	*SINGLE_OPTIONAL_STRING*

continues on next page

Tabulka 1 – pokračujte na předchozí stránce

Údaj	Indentifikátor *claim*u	Datový typ
Příznak – Adresa ověřena *Pouze pro Plný přístup* (`"true"/"false"`) Od července 2022 příznak nelze získat u nových osobních účtů, protože je nelze ověřit pomocí PIN3.	mojeid_address_mail_verified	*SINGLE_OPTIONAL_BOOLEAN*
Fakturační adresa		
Kompletní adresa	mojeid_address_bill	*OPTIONAL_ADDRESS_STRING*
Ulice	mojeid_address_bill_street	*SINGLE_OPTIONAL_STRING*
Ulice 2	mojeid_address_bill_street2	*SINGLE_OPTIONAL_STRING*
Ulice 3	mojeid_address_bill_street3	*SINGLE_OPTIONAL_STRING*
Město	mojeid_address_bill_city	*SINGLE_OPTIONAL_STRING*
Stát	mojeid_address_bill_state	*SINGLE_OPTIONAL_STRING*
PSČ	mojeid_address_bill_postal_code	*SINGLE_OPTIONAL_STRING*
Země	mojeid_address_bill_country	*SINGLE_OPTIONAL_STRING*
Doručovací adresa		
Kompletní adresa	mojeid_address_ship	*OPTIONAL_ADDRESS_STRING*
Jméno společnosti	mojeid_address_ship_company_name	*SINGLE_OPTIONAL_STRING*
Ulice	mojeid_address_ship_street	*SINGLE_OPTIONAL_STRING*
Ulice 2	mojeid_address_ship_street2	*SINGLE_OPTIONAL_STRING*
Ulice 3	mojeid_address_ship_street3	*SINGLE_OPTIONAL_STRING*
Město	mojeid_address_ship_city	*SINGLE_OPTIONAL_STRING*
Stát	mojeid_address_ship_state	*SINGLE_OPTIONAL_STRING*
PSČ	mojeid_address_ship_postal_code	*SINGLE_OPTIONAL_STRING*
Země	mojeid_address_ship_country	*SINGLE_OPTIONAL_STRING*
Telefon		
Mobil	phone_number	*SINGLE_OPTIONAL_STRING*
Příznak – Mobil ověřen (`"true"/"false"`)	phone_number_verified	*SINGLE_OPTIONAL_BOOLEAN*
Další	mojeid_phone_mobile	*SINGLE_OPTIONAL_STRING*
Domácí	mojeid_phone_home	*SINGLE_OPTIONAL_STRING*
Pracovní	mojeid_phone_office	*SINGLE_OPTIONAL_STRING*
Fax	mojeid_phone_fax	*SINGLE_OPTIONAL_STRING*
Další údaje		
Datum narození	birthdate	*SINGLE_OPTIONAL_STRING*

continues on next page

Tabulka 1 – pokračujte na předchozí stránce

Údaj	Indentifikátor *claim*u	Datový typ
Pohlaví	gender	*SINGLE_OPTIONAL_STRING*
Věk	mojeid_age	*SINGLE_OPTIONAL_INT*
Číslo OP	mojeid_ident_card	*SINGLE_OPTIONAL_STRING*
Číslo pasu	mojeid_ident_pass	*SINGLE_OPTIONAL_STRING*
Identifikátor MPSV	mojeid_ident_ssn	*SINGLE_OPTIONAL_STRING*
Číslo ISIC *Pouze pro Plný přístup*	mojeid_isic	*SINGLE_OPTIONAL_STRING*
Příznak – Starší 18 let (`"true"`/`"false"`)	mojeid_is_adult	*SINGLE_OPTIONAL_BOOLEAN*
Příznak – Student *Pouze pro Plný přístup* (`"true"`/`"false"`)	mojeid_student	*SINGLE_OPTIONAL_BOOLEAN*
Příznak – Validace *Pouze pro Plný přístup* (`"true"`/`"false"`)	mojeid_valid	*SINGLE_OPTIONAL_BOOLEAN*
Organizace	mojeid_organization	*SINGLE_OPTIONAL_STRING*
DIČ	mojeid_vat	*SINGLE_OPTIONAL_STRING*
IČO	mojeid_ident_vat	*SINGLE_OPTIONAL_STRING*
Veřejný PGP klíč	mojeid_public_pgp	*SINGLE_OPTIONAL_STRING*
Bankovní účet	mojeid_bank_account	*SINGLE_OPTIONAL_STRING*
Bankovní účet (IBAN)	mojeid_bank_account_iban	*SINGLE_OPTIONAL_STRING*
Datová schránka	mojeid_isds	*SINGLE_OPTIONAL_STRING*
Příznak - NIA *Pouze pro Plný přístup* (`"true"`/`"false"`)	mojeid_nia	*SINGLE_OPTIONAL_BOOLEAN*
URL		
Hlavní	profile	*SINGLE_OPTIONAL_STRING*
Osobní	website	*SINGLE_OPTIONAL_STRING*
Blog	mojeid_url_blog	*SINGLE_OPTIONAL_STRING*
Pracovní	mojeid_url_office	*SINGLE_OPTIONAL_STRING*
RSS	mojeid_url_rss	*SINGLE_OPTIONAL_STRING*
Facebook	mojeid_url_facebook	*SINGLE_OPTIONAL_STRING*
Twitter	mojeid_url_twitter	*SINGLE_OPTIONAL_STRING*
LinkedIN	mojeid_url_linkedin	*SINGLE_OPTIONAL_STRING*
instagram	mojeid_url_instagram	*SINGLE_OPTIONAL_STRING*
pinterest	mojeid_url_pinterest	*SINGLE_OPTIONAL_STRING*
tumblr	mojeid_url_tumblr	*SINGLE_OPTIONAL_STRING*
wordpress	mojeid_url_wordpress	*SINGLE_OPTIONAL_STRING*
foursquare	mojeid_url_foursquare	*SINGLE_OPTIONAL_STRING*
youtube	mojeid_url_youtube	*SINGLE_OPTIONAL_STRING*

continues on next page

Tabulka 1 – pokračujte na předchozí stránce

Údaj	Indentifikátor *claim*u	Datový typ
blogger	mojeid_url_blogger	*SINGLE_OPTIONAL_STRING*
gravatar	mojeid_url_gravatar	*SINGLE_OPTIONAL_STRING*
about_me	mojeid_url_about_me	*SINGLE_OPTIONAL_STRING*
Flickr	mojeid_url_flickr	*SINGLE_OPTIONAL_STRING*
Vimeo	mojeid_url_vimeo	*SINGLE_OPTIONAL_STRING*
IM		
ICQ	mojeid_im_icq	*SINGLE_OPTIONAL_STRING*
Skype	mojeid_im_skype	*SINGLE_OPTIONAL_STRING*
Jabber	mojeid_im_jabber	*SINGLE_OPTIONAL_STRING*
Hangouts	mojeid_im_google_talk	*SINGLE_OPTIONAL_STRING*
Windows Live	mojeid_im_windows_live	*SINGLE_OPTIONAL_STRING*

SINGLE_OPTIONAL_BOOLEAN
Boolean nebo *null*

SINGLE_OPTIONAL_INT
Celé číslo nebo *null*

SINGLE_OPTIONAL_STRING
Řetězec nebo *null*

OPTIONAL_ADDRESS
Objekt nebo *null*

Výpis 1: Schéma objektu OPTIONAL_ADDRESS

```
{
   "formatted": SINGLE_OPTIONAL_STRING,
   "street_address": SINGLE_OPTIONAL_STRING,
   "locality": SINGLE_OPTIONAL_STRING,
   "region": SINGLE_OPTIONAL_STRING,
   "postal_code": SINGLE_OPTIONAL_STRING,
   "country": SINGLE_OPTIONAL_STRING,
}
```

OPTIONAL_ADDRESS_STRING
Řetězec nebo *null*; řetězec obsahuje serializovaný objekt *OPTIONAL_ADDRESS*, např. `"{\"formatted\": \"Pražská 5, Praha\"}"`.

9.2 Příloha č. 3 – Seznam údajů pro předání (SAML)

Tabulka 2: Obecné identifikátory

Údaj	Identifikátor (URI formát)	Identifikátor (BASIC formát)
Jméno		
Celé jméno	urn:oid:2.5.4.3	urn:mace:dir:attribute-def:cn
Křestní jméno	urn:oid:2.5.4.42	urn:mace:dir:attribute-def:givenName
Příjmení	urn:oid:2.5.4.4	urn:mace:dir:attribute-def:sn
Přezdívka	urn:oid:2.5.4.65	urn:mace:dir:attribute-def:pseudonym
E-mail		
Hlavní	urn:oid:0.9.2342.19200300.100.1.3	urn:mace:dir:attribute-def:mail
Adresa trvalého bydliště / sídla firmy		
Kompletní adresa	urn:oid:2.5.4.16	urn:mace:dir:attribute-def:postalAddress
Ulice	urn:oid:2.5.4.9	urn:mace:dir:attribute-def:street
Město	urn:oid:2.5.4.7	urn:mace:dir:attribute-def:l
Stát	urn:oid:2.5.4.8	urn:mace:dir:attribute-def:st
Země	urn:oid:2.5.4.6	urn:mace:dir:attribute-def:c
PSČ	urn:oid:2.5.4.17	urn:mace:dir:attribute-def:postalCode
Telefon		
Mobil	urn:oid:2.5.4.20	urn:mace:dir:attribute-def:telephoneNumber
Fax	urn:oid:2.5.4.23	urn:mace:dir:attribute-def:facsimileTelephoneNumber
Další údaje		
Datum narození	urn:oid:1.3.6.1.4.1.2428.90.1.3	urn:mace:dir:attribute-def:norEduPersonBirthDate
Věk	http://www.stork.gov.eu/1.0/age	
Pohlaví	urn:oid:1.3.6.1.4.1.25178.1.2.2	

continues on next page

Tabulka 2 – pokračujte na předchozí stránce

Údaj	Identifikátor (URI formát)	Identifikátor (BASIC formát)
Obrázek (base64)		urn:mace:dir:attribute-def:photo
Jméno společnosti	urn:oid:2.5.4.10	urn:mace:dir:attribute-def:o
URL		
Hlavní	urn:oid:1.3.6.1.4.1.27630.2.1.1.17	
Pracovní	urn:oid:1.3.6.1.4.1.27630.2.1.1.120	

Tabulka 3: eduID identifikátory

Údaj	Identifikátor (URI formát)
eduID	
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
eduPersonUniqueId	urn:oid:1.3.6.1.4.1.5923.1.1.1.13

9.3 Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)

Tabulka 4: specs.nic.cz identifikátory

Údaj	Identifikátor
Jméno	
Celé jméno	http://specs.nic.cz/attr/contact/name
Křestní jméno	http://specs.nic.cz/attr/contact/name/first
Příjmení	http://specs.nic.cz/attr/contact/name/last
Přezdívka	http://specs.nic.cz/attr/contact/nickname
E-mail	
Hlavní	http://specs.nic.cz/attr/email/main
Notifikační	http://specs.nic.cz/attr/email/notify
Další	http://specs.nic.cz/attr/email/next
Adresa trvalého bydliště / sídla firmy	
Ulice	http://specs.nic.cz/attr/addr/main/street
Ulice2	http://specs.nic.cz/attr/addr/main/street2
Ulice3	http://specs.nic.cz/attr/addr/main/street3
Město	http://specs.nic.cz/attr/addr/main/city
Stát	http://specs.nic.cz/attr/addr/main/sp
Země	http://specs.nic.cz/attr/addr/main/cc
PSČ	http://specs.nic.cz/attr/addr/main/pc
Korespondenční adresa	
Ulice	http://specs.nic.cz/attr/addr/mail/street
Ulice2	http://specs.nic.cz/attr/addr/mail/street2
Ulice3	http://specs.nic.cz/attr/addr/mail/street3
Město	http://specs.nic.cz/attr/addr/mail/city
Stát	http://specs.nic.cz/attr/addr/mail/sp
Země	http://specs.nic.cz/attr/addr/mail/cc
PSČ	http://specs.nic.cz/attr/addr/mail/pc
Příznak – Adresa ověřena *Pouze pro Plný přístup* (`"0"`/`"1"`/`"true"`/`"false"`) Od července 2022 příznak nelze získat u nových osobních účtů, protože je nelze ověřit pomocí PIN3.	http://specs.nic.cz/attr/addr/mail/verified
Fakturační adresa	
Ulice	http://specs.nic.cz/attr/addr/bill/street
Ulice2	http://specs.nic.cz/attr/addr/bill/street2
Ulice3	http://specs.nic.cz/attr/addr/bill/street3
Město	http://specs.nic.cz/attr/addr/bill/city
Stát	http://specs.nic.cz/attr/addr/bill/sp
Země	http://specs.nic.cz/attr/addr/bill/cc

continues on next page

Tabulka 4 – pokračujte na předchozí stránce

Údaj	Identifikátor
PSČ	http://specs.nic.cz/attr/addr/bill/pc
Doručovací adresa	
Firma	http://specs.nic.cz/attr/addr/ship/company_name
Ulice	http://specs.nic.cz/attr/addr/ship/street
Ulice2	http://specs.nic.cz/attr/addr/ship/street2
Ulice3	http://specs.nic.cz/attr/addr/ship/street3
Město	http://specs.nic.cz/attr/addr/ship/city
Stát	http://specs.nic.cz/attr/addr/ship/sp
Země	http://specs.nic.cz/attr/addr/ship/cc
PSČ	http://specs.nic.cz/attr/addr/ship/pc
Telefon	
Mobil	http://specs.nic.cz/attr/phone/main
Další	http://specs.nic.cz/attr/phone/mobile
Domácí	http://specs.nic.cz/attr/phone/home
Pracovní	http://specs.nic.cz/attr/phone/work
Fax	http://specs.nic.cz/attr/phone/fax
Další údaje	
Datum narození	http://specs.nic.cz/attr/contact/ident/dob
Věk	http://specs.nic.cz/attr/contact/age
Pohlaví	http://specs.nic.cz/attr/contact/gender
Číslo OP	http://specs.nic.cz/attr/contact/ident/card
Číslo pasu	http://specs.nic.cz/attr/contact/ident/pass
Identifikátor MPSV	http://specs.nic.cz/attr/contact/ident/ssn
Číslo ISIC *Pouze pro Plný přístup*	http://specs.nic.cz/attr/contact/isic
Příznak – Starší 18 let (`"0"`/`"1"`/`"true"`/`"false"`)	http://specs.nic.cz/attr/contact/adult
Příznak – Student *Pouze pro Plný přístup* (`"0"`/`"1"`/`"true"`/`"false"`)	http://specs.nic.cz/attr/contact/student
Příznak – Validace *Pouze pro Plný přístup* (`"0"`/`"1"`/`"true"`/`"false"`)	http://specs.nic.cz/attr/contact/valid
Stav účtu *Pouze pro Plný přístup*	http://specs.nic.cz/attr/contact/status
Obrázek (base64)	http://specs.nic.cz/attr/contact/image
Jméno společnosti	http://specs.nic.cz/attr/contact/org
IČO	http://specs.nic.cz/attr/contact/ident/vat_id
DIČ	http://specs.nic.cz/attr/contact/vat
Veřejný PGP klíč	http://specs.nic.cz/attr/public_pgp
Bankovní účet	http://specs.nic.cz/attr/bank/national
Bankovní účet (IBAN)	http://specs.nic.cz/attr/bank/iban
Datová schránka	http://specs.nic.cz/attr/contact/isds

continues on next page

Tabulka 4 – pokračujte na předchozí stránce

Údaj	Identifikátor
Příznak - NIA *Pouze pro Plný přístup* (`"0"`/`"1"`/`"true"`/`"false"`)	http://specs.nic.cz/attr/contact/nia
Internetové adresy	
Hlavní	http://specs.nic.cz/attr/url/main
Blog	http://specs.nic.cz/attr/url/blog
Osobní	http://specs.nic.cz/attr/url/personal
Pracovní	http://specs.nic.cz/attr/url/work
RSS	http://specs.nic.cz/attr/url/rss
Facebook	http://specs.nic.cz/attr/url/facebook
Twitter	http://specs.nic.cz/attr/url/twitter
LinkedIN	http://specs.nic.cz/attr/url/linkedin
instagram	http://specs.nic.cz/attr/url/instagram
pinterest	http://specs.nic.cz/attr/url/pinterest
tumblr	http://specs.nic.cz/attr/url/tumblr
wordpress	http://specs.nic.cz/attr/url/wordpress
foursquare	http://specs.nic.cz/attr/url/foursquare
youtube	http://specs.nic.cz/attr/url/youtube
blogger	http://specs.nic.cz/attr/url/blogger
gravatar	http://specs.nic.cz/attr/url/gravatar
about_me	http://specs.nic.cz/attr/url/about_me
Flickr	http://specs.nic.cz/attr/url/flickr
Vimeo	http://specs.nic.cz/attr/url/vimeo
Instant Messaging	
ICQ	http://specs.nic.cz/attr/im/icq
Skype	http://specs.nic.cz/attr/im/skype
Jabber	http://specs.nic.cz/attr/im/jabber
Hangouts	http://specs.nic.cz/attr/im/google_talk
Windows Live	http://specs.nic.cz/attr/im/windows_live

9.4 Příloha č. 5 – Seznam údajů pro registraci

Údaj	Formát	Registrace
Jméno		
Křestní jméno	řetězec o maximální délce 50 znaků	first_name
Příjmení	řetězec o maximální délce 50 znaků	last_name
E-mail		
Hlavní	e-mailová adresa o maximální délce 200 znaků *STD-EMAIL*	email__default__email
Notifikační	e-mailová adresa o maximální délce 200 znaků *STD-EMAIL*	email__notify__email
Další	e-mailová adresa o maximální délce 200 znaků *STD-EMAIL*	email__next__email
Adresa trvalého bydliště / sídla firmy		
Ulice	řetězec o maximální délce 200 znaků	address__default__street1
Ulice2	řetězec o maximální délce 200 znaků	address__default__street2
Ulice3	řetězec o maximální délce 200 znaků	address__default__street3
Město	řetězec o maximální délce 200 znaků	address__default__city
Stát	řetězec o maximální délce 200 znaků	address__default__state
PSČ	řetězec o maximální délce 50 znaků	address__default__postal_code
Země	kód země podle ISO3166 *STD-COUNTRY*	address__default__country
Fakturační adresa		
Ulice	řetězec o maximální délce 200 znaků	address__billing__street1
Ulice2	řetězec o maximální délce 200 znaků	address__billing__street2
Ulice3	řetězec o maximální délce 200 znaků	address__billing__street3
Město	řetězec o maximální délce 200 znaků	address__billing__city
Stát	řetězec o maximální délce 200 znaků	address__billing__state
PSČ	řetězec o maximální délce 50 znaků	address__billing__postal_code
Země	kód země podle ISO3166 *STD-COUNTRY*	address__billing__country

continues on next page

Tabulka 5 – pokračujte na předchozí stránce

Údaj	Formát	Registrace
Doručovací adresa		
Firma	řetězec o maximální délce 200 znaků	address__shipping__company_name
Ulice	řetězec o maximální délce 200 znaků	address__shipping__street1
Ulice2	řetězec o maximální délce 200 znaků	address__shipping__street2
Ulice3	řetězec o maximální délce 200 znaků	address__shipping__street3
Město	řetězec o maximální délce 200 znaků	address__shipping__city
Stát	řetězec o maximální délce 200 znaků	address__shipping__state
PSČ	řetězec o maximální délce 50 znaků	address__shipping__postal_code
Země	kód země podle ISO3166 *STD-COUNTRY*	address__shipping__country
Korespondenční adresa		
Ulice	řetězec o maximální délce 200 znaků	address__mailing__street1
Ulice2	řetězec o maximální délce 200 znaků	address__mailing__street2
Ulice3	řetězec o maximální délce 200 znaků	address__mailing__street3
Město	řetězec o maximální délce 200 znaků	address__mailing__city
Stát	řetězec o maximální délce 200 znaků	address__mailing__state
PSČ	řetězec o maximální délce 50 znaků	address__mailing__postal_code
Země	kód země podle ISO3166 *STD-COUNTRY*	address__mailing__country
Telefon		
Mobil	řetězec odpovídající regulárnímu výrazu: ^+[0-9]{1,3}.[0-9]{1,14}$	phone__default__number
Pracovní	řetězec odpovídající regulárnímu výrazu: ^+[0-9]{1,3}.[0-9]{1,14}$	phone__office__number
Další	řetězec odpovídající regulárnímu výrazu: ^+[0-9]{1,3}.[0-9]{1,14}$	phone__mobile__number
Domácí	řetězec odpovídající regulárnímu výrazu: ^+[0-9]{1,3}.[0-9]{1,14}$	phone__home__number

continues on next page

Tabulka 5 – pokračujte na předchozí stránce

Údaj	Formát	Registrace
Telefon - Fax	řetězec odpovídající regulárnímu výrazu: ^+[0-9]{1,3}.[0-9]{1,14}$	phone__fax__number
Další údaje		
Datum narození	datum ve formátu RFC3339 (YYYY-MM-DD) *STD-DATE*	birth_date
Pohlaví	hodnota „M“ nebo „F“	gender
Číslo OP	řetězec o maximální délce 50 znaků	id_card_num
Číslo pasu	řetězec o maximální délce 50 znaků	passport_num
Identifikátor MPSV	řetězec o maximální délce 50 znaků	ssn_id_num
Číslo ISIC	řetězec o maximální délce 50 znaků	card_isic
Jméno společnosti	řetězec o maximální délce 200 znaků	organization
IČO	řetězec o maximální délce 50 znaků	vat_id_num
DIČ	řetězec o maximální délce 50 znaků	vat_reg_num
Internetové adresy		
Hlavní	řetězec o maximální délce 255 znaků	urladdress__main__url
Blog	řetězec o maximální délce 255 znaků	urladdress__blog__url
Osobní	řetězec o maximální délce 255 znaků	urladdress__personal__url
Pracovní	řetězec o maximální délce 255 znaků	urladdress__office__url
RSS	řetězec o maximální délce 255 znaků	urladdress__rss__url
Facebook	řetězec o maximální délce 255 znaků	urladdress__facebook__url
Twitter	řetězec o maximální délce 255 znaků	urladdress__twitter__url
LinkedIN	řetězec o maximální délce 255 znaků	urladdress__linkedin__url
instagram	řetězec o maximální délce 255 znaků	urladdress__instagram__url
pinterest	řetězec o maximální délce 255 znaků	urladdress__pinterest__url
tumblr	řetězec o maximální délce 255 znaků	urladdress__tumblr__url
wordpress	řetězec o maximální délce 255 znaků	urladdress__wordpress__url
foursquare	řetězec o maximální délce 255 znaků	urladdress__foursquare__url

continues on next page

Tabulka 5 – pokračujte na předchozí stránce

Údaj	Formát	Registrace
youtube	řetězec o maximální délce 255 znaků	urladdress__youtube__url
blogger	řetězec o maximální délce 255 znaků	urladdress__blogger__url
gravatar	řetězec o maximální délce 255 znaků	urladdress__gravatar__url
about_me	řetězec o maximální délce 255 znaků	urladdress__about_me__url
Instant Messaging		
ICQ	řetězec o maximální délce 255 znaků	imaccount__icq__username
Skype	řetězec o maximální délce 255 znaků	imaccount__skype__username
Windows Live	řetězec o maximální délce 255 znaků	imaccount__windows_live__username
Jabber	řetězec o maximální délce 255 znaků	imaccount__jabber__username
Hangouts	řetězec o maximální délce 255 znaků	imaccount__google_talk__username

STD-EMAIL

E-mailová adresa ve formátu podle **RFC 2822**[65]

STD-COUNTRY

Kód země podle ISO 3166[66]

STD-DATE

Datum ve formátu **RFC 3339**[67]

[65] https://datatracker.ietf.org/doc/html/rfc2822.html
[66] https://www.iso.org/iso-3166-country-codes.html
[67] https://datatracker.ietf.org/doc/html/rfc3339.html

9.5 Příloha č. 6 – Příklady a řešení chybových hlášek

Následující článek popisuje nejčastější chybové hlášky, které při implementaci MojeID mohou vzniknout. V textu jsou dále popsána doporučení, jak chybu řešit, případně na co se zaměřit.

9.5.1 Chybové hlášky na testovací instanci

Chyby se vypisují přímo z použitých knihoven. Zde jsou vypsány ty nejdůležitější:

- *„Error parsing document as XML“* a *„Not a XRDS document“* – Obojí znamená chybný XRDS dokument. Tato hláška obvykle značí problém v XRDS dokumentu, že XML kód není validní (nejčastěji kvůli obsahu nestandardních unicode znaků). Na adrese http://www.xmlvalidation.com je možné si zdrojový kód překontrolovat a zjistit tak, kde se chyba nachází.
- *„No XRD present in tree“* – XRDS dokument nemá žádný XRD element. Překontrolujte obsah XRDS dokumentu, viz sekci xrds. Pozor také na velikost písmen ve značkách!
- *„HTTP Response status from identity URL host is not 200. Got status XXX“* – dotaz na *realm* nebo XRDS dokument vrátil stavový kód HTTP jiný než 200.
- Chyby z cURLu jsou ve tvaru *„(XX, ...)“*, kde XX je číslo chyby ze seznamu chyb libcURL viz https://curl.haxx.se/libcurl/c/libcurl-errors.html

9.5.2 Problémy s ověřením návratové adresy

V případě, že se nepodaří ověřit návratovou adresu služby, je zobrazena uživateli některá z následujících zpráv podle toho, ve které fázi došlo k negativnímu výsledku:

a. **Pokud se nepodařilo spojit se službou**

   „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.“

   Tato hláška je zobrazena, pokud dotaz na *realm* nebo dokument XRDS vrátil stavový kód HTTP 4xx nebo 5xx. Pokud to není ten případ, může hláška značit problém s certifikátem při použití HTTPS.

   Pro správné fungování HTTPS je třeba mít platný certifikát, který si můžete pořídit od certifikační autority (viz také *Problém s nezašifrovaným spojením* (str. 79)). Zároveň musíte mít i tzv. *intermediate* certifikáty, aby vůbec došlo k hledání XRDS dokumentu. Musí být správně nastaven serverový certifikát, např. na serveru Apache se *intermediate* certifikáty nastaví pomocí direktivy `SSLCertificateChainFile`, příp. `SSLCertificateFile`, viz dokumentaci nastavení SSL v Apache[68].

   Přehled certifikačních autorit, které MojeID podporuje, naleznete na adrese: https://wiki.mozilla.org/CA/Included_Certificates

   Při odlaďování problémů se SSL a certifikáty vám mohou pomoci přímé nástroje, např. programy `wget` nebo `curl`, případně nějaký mechanismus použité knihovny, které umí potíže odhalit lépe než běžné prohlížeče.

[68] https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatechainfile

b. **Pokud se podařilo spojit se službou, 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.“

Selhání při ověření návratové adresy může nastávat z těchto příčin:

- *Realm* nevrátil stavový kód HTTP 200.
- Na *realmu* se nenachází XRDS dokument, nemůže tak dojít k ověření služby. Umístění XRDS dokumentu na *realmu* musí být jedním ze tří způsobů:
  - XRDS dokument se může nacházet přímo v HTTP hlavičce
  - XRDS dokument může být uložen přímo na adrese *realmu* (zaslán přímo v odpovědi)
  - umístění může být uvedeno v hlavičce HTML ve značce META
- Během procesu stahování XRDS dokumentu se objevilo přesměrování.
- Když nesedí adresa `return_to` v OpenID požadavku s adresou `return_to` v XRDS dokumentu. Adresa `return_to` z OpenID požadavku může obsahovat navíc pouze další parametry, tzv. *query string*, **nikoli podadresáře v cestě**.
- Když adresa `return_to` z OpenID požadavku „není rozšířením“ adresy *realmu*.

  Pojem *adresa A „je rozšířením“ adresy B* znamená, že:
  - protokol je stejný,
  - doména je stejná nebo navíc obsahuje poddoménu, pokud doména B začíná na `*.`,
  - port je stejný,
  - cesta je stejná nebo obsahuje podadresáře, a
  - *query string* (?klic=hodnota&klic2=hodnota2) stejný nebo s parametry navíc.

Tabulka 6: Příklady: adresa A „je rozšířením“ adresy B

Platnost tvrzení	Adresa A	Adresa B
Ano	https://example.com/ahoj/	https://example.com/ahoj/
Ne	http://example.com/ahoj/	https://example.com/ahoj/
Ne	https://example.com:8080/ahoj/	https://example.com/ahoj/
Ano	https://example.com/ahoj/cau/	https://example.com/ahoj/
Ne	https://example.com/ahoj/	https://example.com/cau/
Ne	https://example.com/ahoj/	https://example.com/ahoj/cau/
Ano	https://example.com/ahoj/ ?klic=hodnota	https://example.com/ahoj/ ?klic=hodnota
Ano	https://example.com/ahoj/ ?klic=hodnota&klic2=hodnota2	https://example.com/ahoj/ ?klic=hodnota
Ne	https://example.com/ahoj/ ?klic=hodnota	https://example.com/ahoj/ ?klic=hodnota&klic2=hodnota2
Ano	https://subdomain.example.com/ahoj/ ?klic=hodnota	https://*.example.com/

c. **Pokud oblast URL služby nelze spravovat v MojeID**

„Tento realm není dobře definovaný a nelze k němu nastavit důvěru.“
„This realm is not sane and thus you can not set trust for it.“

Ověřte, že váš *realm* (uvedený v žádosti o ověření identity) neobsahuje IP adresu, pro URL nepovolené znaky nebo URI fragment[69]. Viz také realm.

9.5.3 Problém s nezašifrovaným spojením

Může se stát, že prohlížeč zobrazí při přesměrování zpět na vaše stránky následující hlášku:

„Informace, které jste zadali, budou odeslány přes nezašifrované spojení a mohly by jednoduše být přečteny třetí stranou. Určitě chcete pokračovat v odesílání?“
„The information you have entered will be sent over an unencrypted connection and could easily be read by a third party. Are you sure you want to continue sending it?“

Poznámka: Uvedená hláška pochází z Firefoxu, v jiných prohlížečích pravděpodobně bude mít odlišné znění.

Toto hlášení se může objevit u všech *realmů* bez HTTPS. Předávané údaje (tj. i uživatelovy osobní údaje) putují po internetu nešifrovaně, a prohlížeč hlásí, že opouští šifrované stránky MojeID směrem ke službě, která šifrování nepoužívá. Nešifrovaný protokol (HTTP) nedoporučujeme, ale chyba to není.

Tento problém se dá snadno vyřešit použitím základního SSL certifikátu, který lze získat např. zde: https://letsencrypt.org/. Certifikát Vám zabezpečí chráněný přenos dat a současně vidíte, jakou úroveň ověření uživatel má.

[69] https://en.wikipedia.org/wiki/Uniform_Resource_Identifier#Generic_syntax

9.5.4 Volba vyžadované přihlašovací metody

Vyžadovaná přihlašovací metoda se zvolí umístěním identifikátoru příslušné přihlašovací metody do žádosti o ověření identity. Služba MojeID podporuje mimo běžného přihlašování heslem i přihlašování pomocí digitálního certifikátu, jednorázového hesla (OTP) nebo bezpečnostního tokenu.

- V případě přihlášení **pomocí certifikátu** se zobrazuje následující hláška:

  „Poskytovatel služby požaduje přihlášení certifikátem.“
  „The service provider wants you to login with your certificate.“

- V případě přihlášení **pomocí jednorázového hesla** nebo **pomocí autentikátoru** se zobrazuje následující hláška:

  „Poskytovatel služby požaduje přihlášení jednorázovým heslem nebo MojeID Autentikátorem.“
  „The service provider wants you to login with one time password or MojeID Autentikátor.“

- V případě přihlášení **pomocí bezpečnostního tokenu** se zobrazuje následující hláška:

  „Poskytovatel služby požaduje přihlášení druhým faktorem.“
  „The service provider wants you to login with two-factor authentication.“

Identifikátory metod a příklad žádosti s vyžádáním přihlašovací metody naleznete v sekci implem-oid2-zadost-overeni.

9.5.5 Problémy s knihovnou pro PHP

Mezi časté chybové hlášky patří zejména *„FAILED TO CREATE AUTH REQUEST: not a valid OpenID“* a *„Ověření OpenID selhalo: No OpenID information“*.

Některé chyby mohou být způsobeny chybnou konfigurací vašeho serveru. Pro jejich nápravu můžete zkusit následující kroky:

- Je zapotřebí se ujistit, že je cURL pro danou verzi PHP nainstalováno, zapnuté (phpinfo by tak mělo hlásit) a že v `php.ini` není cURL zakázáno.
- Případně může být třeba do souboru `/etc/php5/conf.d/curl.ini` uvést řádek `extension=curl.so`, pokud tam není.
- Stáhněte si a nainstalujte nejnovější verzi cURL viz https://curl.haxx.se/download.html.

Dále Vám doporučujeme stáhnout a prostudovat si vzorovou implementaci v PHP.

9.5.6 Chybové odpovědi v JSONu (OIDC)

Chybové odpovědi obsahují kód chyby pod klíčem `error` ve formě ASCII řetězce. Lidsky čitelný popis chyby by se měl vyskytovat v JSON odpovědi pod klíčem `error_description`.

Chybové kódy, které může MojeID vrátit:

Kód chyby	Možné příčiny
`unauthorized_client`	Špatné `client_id`, špatné `client_secret`, špatně použitá autentifikace.
`invalid_request`	Chybějící povinné parametry, některý parametr nečitelný/neparsovatelný.

9.6 Příloha č. 7 – Zásady správné implementace

Při implementaci podpory služby MojeID dodržujte následující zásady:

1. Přihlášení ke službě MojeID realizujte výhradně tlačítkem „Přihlásit přes MojeID“ dle vzoru v sekci implem-oid-zadost-prihlaseni.

2. Tlačítko „Přihlásit přes MojeID“ vhodně doplňte textovými odkazy „Proč MojeID?“ a „Založit účet MojeID“.

   a. Odkaz „Proč MojeID?“ nasměrujte na lokální stránku vysvětlující výhody využití MojeID na vašich stránkách (lokální výhody) nebo na informační stránku služby MojeID[70].

   b. Odkaz „Založit účet MojeID“ můžete nahradit tlačítkem „Založit účet MojeID“ dle vzoru.

   Tlačítko nasměrujte na lokální registrační stránku MojeID nebo na univerzální registrační formulář[71] služby MojeID .

   c. Pokud není možné doplnit tlačítko odkazy podle předchozích bodů (2.a a 2.b), doporučujeme přidat je na stránku administrace lokálního účtu uživatele.

3. Pokud je to možné, umístěte na hlavní stránku logo „Podporuje MojeID“ dle vzoru s odkazem na místo ve vašem systému, kde je MojeID použito nebo na lokální stránku ve vašem systému s informací o službě MojeID.

[70] https://www.mojeid.cz/cs/proc-mojeid/
[71] https://mojeid.cz/registration/

4. Požadované údaje pro předání musí být v souladu s vaším systémem:
    a. jako povinné musí být označeny pouze položky, které jsou povinné pro registrační proces ve vašem systému,
    b. ostatní požadované položky musí být označeny jako nepovinné,
    c. nesmíte požadovat k předání položky, které nevyužíváte v systému.
5. Pokud při přihlášení přes MojeID vyžadujete předání údajů o uživateli, je – v případě, že se tyto údaje liší od údajů evidovaných v lokálním účtu vaší služby – doporučeno dát uživateli na výběr, zdali si přeje stávající údaje v lokálním účtu služby ponechat, nebo zda mají být přepsány údaji přenesenými z MojeID.
6. Implementace služby MojeID musí být navržena tak, aby uživatel MojeID měl při svém prvním přístupu k vaší službě prostřednictvím MojeID na výběr z následujících dvou možností:
    a. spárování MojeID s existujícím lokálním účtem, nebo
    b. vytvoření nového lokálního účtu pomocí dat přenesených z MojeID a spárování tohoto nově založeného lokálního účtu s MojeID.
7. V administraci lokálního účtu uživatele:
    a. doporučujeme při spárování s účtem MojeID zobrazit MojeID identifikátor uživatele,
    b. doporučujeme mít odkaz nebo tlačítko „Založit účet MojeID“ podle bodu 2. V případě, že uživatel ještě nemá spárovaný lokální účet s MojeID, a tedy pravděpodobně nemá MojeID, doporučujeme registrační formulář MojeID předvyplnit údaji z lokálního účtu uživatele,

    c. musí mít uživatel možnost spárovat MojeID s existujícím lokálním účtem, pokud již není spárován.
    d. uživatel musí mít možnost odpojit lokální účet od účtu MojeID.
8. Úpravy vzhledu tlačítek a dalších grafických prvků jsou možné jen s výslovným souhlasem sdružení CZ.NIC.
9. Implementace MojeID musí být realizována výhradně na protokoli OpenID Connect nebo SAML dle specifikace v technické dokumentaci

Varování: Protokol OpenID 2.0 již není podporován.

Kapitola 10

Přehled změn

Verze	Segment	Popis změny
3.1.4	*Kontrola validity dat* (str. 51)	Upraven návod o zaslání klientského certifikátu
	Celá dokumentace	Odebrání posledních zmínek o protokolu OpenID 2.0
3.1.3	*Přihlášení k MojeID pomocí PHP klienta* (str. 30)	Přidán plugin pro ukázkové přihlášení k MojeID pomocí PHP klienta
3.1.2	*Kontrola validity dat* (str. 51) *Dokončení registrace* (str. 53) *Testovací instance MojeID* (str. 57) *Přehled knihoven a modulů* (str. 16)	Úpavy dokumentace spojené se zrušením ověřování pomocí PIN1 a PIN2
3.1.1	*Žádost o ověření identity účtem napojeným na NIA* (str. 46) *Implementace pomocí SAML* (str. 47)	Oprava hodnot *acr_values* a *AuthnContextClassRef* včetně příkladu použití
	MojeID plugin pro WordPress (str. 16)	Aktualizace návodu pro přihlášení účtem napojeným na NIA
3.1	Celá dokumentace	Odstraněny všechny části dokumentace o protokolu OpenID 2.0
3.0.9	*Přehled knihoven a modulů* (str. 16)	Přidány návody na instalaci rozšíření pro populární platformy (pouze CS verze dokumentace)
3.0.8	*Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62)	Doplněn předávaný údaj „Organizace“ u OIDC Opraveny prohozené pojmy DIČ a IČO
	Příloha č. 6 – Příklady a řešení chybových hlášek (str. 76)	Změněn odkaz u SSL certifikátu na certifikační službu Let's Encrypt
	Registrace klienta (str. 35) *Knihovna MojeID LITE* (str. 44)	Doplněna poznámka, že automatickou (dynamickou) registraci nelze využít pro plný přístup
3.0.7	Celá dokumentace	Přejmenování `mojeID` na `MojeID` Aktualizace obrázků a tlačítek Oprava zastaralých a neplatných odkazů
3.0.6	*Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62) `/Prilohy/UdajePredaniOID/index` *Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69) *Dokončení registrace* (str. 53) *Testovací instance MojeID* (str. 57)	Odebrána možnost ověření účtů fyzických osob pomocí PIN3 Doplněna informace „*Pouze pro Plný přístup*“ u Korespondenční adresy

continues on next page

Tabulka 1 – pokračujte na předchozí stránce

Verze	Segment	Popis změny
3.0.5	*Základní principy MojeID* (str. 7) *Napojení MojeID na NIA* (str. 14) *Žádost o ověření identity účtem napojeným na NIA* (str. 46) *Implementace pomocí SAML* (str. 47)	Přidány informace o napojení mojeID na NIA
3.0.4	`/SeznameniSMojeid/ProcesKomunikaceRozdilyMezi` a všechny podkapitoly *Favikona* (str. 12) `/ImplementacePodporyMojeid/OpenIdConnect` a všechny podkapitoly *Testovací instance MojeID* (str. 57) `/Prilohy/UdajePredaniOID/index`	Přidány varování o plánovaném ukončení podpory protokolu OpenID 2.0 na všechny relevantní stránky
3.0.3	*Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62) `/Prilohy/UdajePredaniOID/index` *Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69)	Přidáno údaj *Příznak - NIA* do seznamu předávaných údajů Změna pojmu *Domácí adresa* na *Adresa trvalého bydliště / sídla firmy*
3.0.2	Celá dokumentace (anglická verze)	Oprava překlepů a nepřeloženého textu
3.0.1	Jen HTML část	Přidány odkazy na jazykové verze Logo dokumentace odkazuje na hlavní stránku webu
	Celá dokumentace (anglická verze)	Pojem „disclose“ změněn na „hand over“ v kontextu předávaných údajů Opraveny některé překlepy
3.0	Celá dokumentace	Přidána anglická verze dokumentace
2.18	*Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62)	Doplněn předávaný údaj „country“ u OIDC
	`/ImplementacePodporyMojeid/OpenIdConnect` *Příloha č. 6 – Příklady a řešení chybových hlášek* (str. 76)	Doplněna varianta přihlášení pomocí bezpečnostního tokenu včetně příslušných uživatelských hlášek
	Proces komunikace přes OpenID Connect (str. 8) `/SeznameniSMojeid/ProcesKomunikacePresMojeid/OpenID/index`	Doplněna přihlašovací metoda – bezpečnostní token
2.17	*Registrace klienta* (str. 35)	Doplněn postup ruční registrace klienta v testovací instanci mojeID pro protokol OIDC
2.16	*Přechod na jiný protokol* (str. 48)	Změna textu sekce Přechod na jiný protokol, přidání konkrétních informací o přechodu z OID2 na OIDC
	Rozdíly mezi protokoly (str. 48)	Přidání mezer kolem lomítka v sekci Implementace pomocí OpenID Connect (OIDC)
	Implementace pomocí OpenID Connect (OIDC) (str. 15)	Oprava dvou velkých písmen pro větší konzistenci v sekci Žádost o ověření identity

continues on next page

Tabulka 1 – pokračujte na předchozí stránce

Verze	Segment	Popis změny
2.15	*Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62) `/Prilohy/UdajePredaniOID/index` *Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69)	Opraveno označení Pro plný přístup u předávaných údajů
2.14	*Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62) `/Prilohy/UdajePredaniOID/index`	Popsány datové typy předávaných údajů
2.13	*Právní upozornění* (str. 1)	Přidáno právní upozornění týkající se dokumentace
	Přehled změn	Přepracován s nejnovějšími změnami nahoře
2.12	*Registrace klienta* (str. 35), *Žádost o data* (str. 43)	Opraveny nevalidní JSON příklady
	Příloha č. 1 – Seznam údajů pro předání (OpenID Connect) (str. 62) `/Prilohy/UdajePredaniOID/index` *Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69) *Příloha č. 5 – Seznam údajů pro registraci* (str. 72)	Odstraněny předávané údaje „Číslo Opencard“ a „google_plus“ u všech protokolů
2.11	Všude	Opraveny odkazy na nové webové stránky mojeID
2.10	*Přehled kroků implementace* (str. 32)	Přidán přehled kroků implementace pomocí OIDC
	Přehled knihoven a modulů (str. 16)	Přidán přehled knihoven a modulů pro OIDC
	`/ImplementacePodporyMojeid/OpenidPrehledKnihoven/index`	Přidán přehled knihoven a modulů pro OID2
2.9	*Favikona* (str. 12)	Vysvětlení účelu favikony a pokyny k jejímu nastavení
	Odhlašování od služby MojeID (str. 55)	Pokyny k možnosti odhlášení
	Příloha č. 6 – Příklady a řešení chybových hlášek (str. 76)	Změněno doporučení k ladění SSL
2.8	*Implementace podpory MojeID* (str. 15)	Důležitá poznámka o zakázaném použití rámců
2.7	*Testovací instance MojeID* (str. 57)	Aktualizovány adresy podle nového testovacího serveru a výslovně vypsány všechny endpointy OIDC
	Všude	Nová adresa na technickou podporu techsupport@mojeid.cz
2.6	Všude	Změněno pořadí protokolů – OIDC jako první
	`/ImplementacePodporyMojeid/OpenidPrehledKnihoven/index`	Změněn název kapitoly
2.5	*Registrace klienta* (str. 35)	Přidána možnost ruční registrace služby v OpenID Connect přes nové rozhraní serveru mojeID
2.4	*Rozhraní pro zakládání účtů MojeID* (str. 51)	Rozšířeno o podporu přímé registrace i přes protokol OpenID Connect

continues on next page

Tabulka 1 – pokračujte na předchozí stránce

Verze	Segment	Popis změny
2.3	*Testovací instance MojeID* (str. 57)	Doplněny informace pro testování komunikace přes protokoly OIDC a SAML
	Implementace pomocí OpenID Connect (OIDC) (str. 15)	Doplněny ukázky kódu a komunikace pro implementaci pomocí protokolu OIDC
	Ladění komunikace se serverem MojeID (str. 48)	Doplněno doporučení k odlaďování komunikace
	Příloha č. 6 – Příklady a řešení chybových hlášek (str. 76)	Přidána zmínka o chybových odpovědích v JSON u OIDC, nahrazen zastaralý odkaz
	`/Prilohy/UdajePredaniOID/index` *Příloha č. 1 – Seznam údajů pro předání (OpenID Connect)* (str. 62) *Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69)	Přidán údaj pro předání – datová schránka (ISDS)
2.2	*Příloha č. 4 – Seznam údajů pro předání (SAML specs.nic.cz)* (str. 69)	Přidán seznam dalších identifikátorů pro předávání údajů přes SAML
2.1	*Základní principy MojeID* (str. 7)	Přesunutí odkazů na specifikace protokolů do `/ImplementacePodporyMojeid/Openid/index` a *Implementace pomocí OpenID Connect (OIDC)* (str. 15)
	Implementace pomocí OpenID Connect (OIDC) (str. 15)	Přidán odkaz na konfiguraci OIDC na serveru mojeID
	Registrace klienta (str. 35)	Přidána zmínka o metadatech klienta a doplňující info k ruční registraci
	Knihovna MojeID LITE (str. 44)	Přidán celý segment
	Implementace pomocí SAML (str. 47)	Přidán odkaz na certifikát pro ověření metadat a na nástroj pro dekódování zpráv SAMLu
	Problémy při implementaci (str. 47)	Přidán celý segment
	Příloha č. 6 – Příklady a řešení chybových hlášek (str. 76)	Přidán odkaz na nástroj k otestování nastavení SSL
	Přehled změn	Přidán celý segment

Rejstřík