

Nástrahy a překvapení implementací MojeID do aplikací třetích stran

Adam Beneš & Jiří Antoň • techsupport@mojeid.cz • 7. října 2023

Obsah přednášky

- Co je to MojeID,
- výhody MojeID jako SSO metody,
- dostupné způsoby implementace,
- možné problémy s vývojem SSO pluginů.



Co je to MojID?

- Poskytovatel elektronické identity:
 - soubor osobních údajů,
 - SSO - jedno uživatelské jméno a heslo,
 - jednoduchá registrace u nových služeb,
- podpora standardů OpenID Connect a SAML.



Výhody MojeID

- Bezpečnost přihlašování,
 - ověření přes HW klíče,
 - úrovně značná a vysoká,
- kontrola nad předávanými údaji,
- možnost ověření pravosti údajů.

Dostupné způsoby implementace - WordPress

- Nejrozšířenější CMS na světě (43 % / 63 %),
 - odpovídá tomu úroveň dokumentace,
- plugin WooCommerce (12 % CZ e-shopů),
- funkční plugin OpenID Connect Generic:
 - client ID a secret,
 - scope, endpointy,
 - klíče zpracování identity,
 - hook pro umístění tlačítka přihlášení.



WordPress - konfigurace

Client ID	
	The ID this client will be recognized as when connecting the to Identity provider server. Example: <code>my-wordpress-client-id</code>
Client Secret Key	
	Arbitrary secret key the server expects from this client. Can be anything, but should be very unique.
OpenID Scope	email openid profile
	Space separated list of scopes this client should access. Example: <code>email profile openid offline_access</code>
Login Endpoint URL	https://mojeid.cz/oidc/authorization/
	Identify provider authorization endpoint. Example: <code>https://example.com/oauth2/authorize</code>
Userinfo Endpoint URL	https://mojeid.cz/oidc/userinfo/
	Identify provider User information endpoint. Example: <code>https://example.com/oauth2/UserInfo</code>
Token Validation Endpoint URL	https://mojeid.cz/oidc/token/
	Identify provider token endpoint. Example: <code>https://example.com/oauth2/token</code>

Identity Key	email
	Where in the user claim array to find the user's identification data. Possible standard values: <code>preferred_username</code> , <code>name</code> , or <code>sub</code> . If you're having trouble, use <code>*sub</code> . Example: <code>preferred_username</code>
Nickname Key	email
	Where in the user claim array to find the user's nickname. Possible standard values: <code>preferred_username</code> , <code>name</code> , or <code>sub</code> . Example: <code>preferred_username</code>
Email Formatting	<input data-kind="parent" data-rs="2" type="text" value="{email}"/>
	String from which the user's email address is built. Specify <code>{email}</code> as long as the user claim contains an email claim. Example: <code>{email}</code>
Display Name Formatting	<input data-kind="parent" data-rs="2" type="text" value="{given_name} {family_name}"/>
	String from which the user's display name is built. Example: <code>{given_name} {family_name}</code>



Dostupné způsoby implementace - WordPress

- NIA Approved Comment plugin:
 - Národní identitní autorita,
 - ukázka možností MojeID,
 - schvalování komentářů jen od existujících lidí.



Require prompt addon



Dostupné způsoby implementace - Drupal

- Funkční OpenID Connect plugin:
 - client ID a secret,
 - scope, endpointy,
 - služba MojID - MR do upstreamu,
 - pouze credentials,
 - potřeba umístit login button,
 - možné problémy s PHP composerem.
 - verze pluginu X verze Drupalu.



Dostupné způsoby implementace - OpenCart

- In-house OpenID Connect plugin:
 - client ID a secret,
 - scope, endpointy,
- obtížná instalace:
 - upload -> potvrzení -> výběr kategorie -> aktivace,
 - vložení tlačítka = úprava TWIG šablon,
 - potřeba nahrát grafické balíčky => sysmaster,
 - login v liště/patičce,
 - problém při renderu.



OpenCart - konfigurace

✎ OpenID Connect settings

Client authentication

• Client ID

• Client secret

Identity provider endpoints

• Authorization endpoint URL

• Token endpoint URL

• Userinfo endpoint URL

Generated data

Redirect URL

Save



Dostupné způsoby implementace - Joomla!

- In-house OpenID Connect plugin:
 - client ID a secret,
 - scope, endpointy,
- instalace i konfigurace velmi jednoduchá,
- lehce obtížné vložení tlačítka,
 - nepodporuje úpravu HTML => modul,
 - obrázek jako odkaz,
 - lze umístit téměř kamkoli.



Joomla! - konfigurace

OpenID Connect setup

Authorization endpoint URL	https://mojeid.cz/oidc/authorization/
Token endpoint URL	https://mojeid.cz/oidc/token/
Userinfo endpoint URL	https://mojeid.cz/oidc/userinfo/
After login URL	index.php URL to navigate to after login.
Client ID	 Client ID as set in the authorization server.
Client secret	 Client secret as set in the authorization server.



Dostupné způsoby implementace - PrestaShop

- Existující plugin, ale closed-source,
- in-house OpenID Connect plugin:
 - client ID a secret,
 - scope, endpointy,
 - instalace i konfigurace velmi jednoduchá,
 - není potřeba umisťovat tlačítko.



IdP name (title)	MojeID
* Client ID	
* Client secret	
Authorization endpoint URL	https://mojeid.cz/oldc/authorization/
Token endpoint URL	https://mojeid.cz/oldc/token/
Userinfo endpoint URL	https://mojeid.cz/oldc/userinfo/
* Scope	openid profile email
Require prompt	☐ Require prompt
Redirect URL	http://.../Index.php?fc=module&module=openidconnect&controller=callback&id_lang=1



Problémy s vývojem obecně



Problémy s vývojem obecně - dokumentace



Problémy s vývojem obecně - dokumentace



Problémy specifické pro OpenCart

- Již existuje rozšíření...



Problémy specifické pro OpenCart

- Již existuje rozšíření... 6 let staré.



Problémy specifické pro OpenCart

- Již existuje rozšíření... 6 let staré.
- Vyšel OpenCart 4...



Problémy specifické pro OpenCart

- Již existuje rozšíření... 6 let staré.
- Vyšel OpenCart 4 a už nepoužívá OCMOD.



Problémy specifické pro OpenCart

- Již existuje rozšíření... 6 let staré.
- Vyšel OpenCart 4 a už nepoužívá OCMOD.
- Název `<plugin>.ocmod.zip`, obsahuje jen soubory.



Problémy specifické pro OpenCart

- Již existuje rozšíření... 6 let staré.
- Vyšel OpenCart 4 a už nepoužívá OCMOD.
- Název <plugin>.ocmod.zip, obsahuje jen soubory.



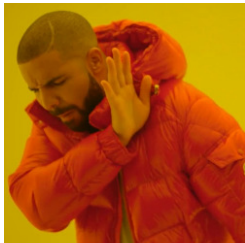
Naše problémy



Naše problémy



Naše problémy



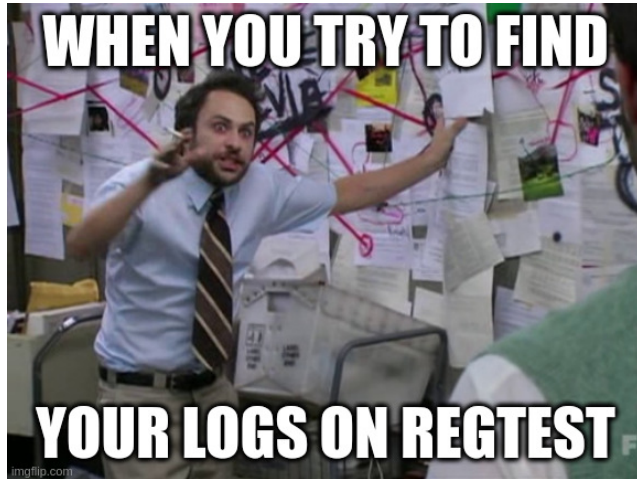
GitLab

Most Recent Activity

-  **Tanya Horne** @TanyaHorne
Opened issue #13 "Download Starfield torrent from Igruhi on PC" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #12 "Starfield (2023) torrent download for PC" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #11 "Starfield Full Game Premium Edition Download on PC Free (CRACK RUNE)" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #10 "Download Starfield Game For PC Free Full Version" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #9 "Starfield Game Free Download For PC Full Version" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #8 "Download Starfield for PC Full Game Cracked RUNE" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #7 "Starfield Download (Last Version) Free PC Game Torrent" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #6 "Starfield - Download Game PC Iso New Free" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #5 "Download Starfield Full Game on PC for FREE" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #4 "Starfield Download Pc Game Full Version Free Download" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #3 "Starfield Download Free PC" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #2 "Starfield Full Version Free Download" at [utils / opencart-openid-connect](#)
-  **Tanya Horne** @TanyaHorne
Opened issue #1 "Starfield Download FULL PC GAME" at [utils / opencart-openid-connect](#)



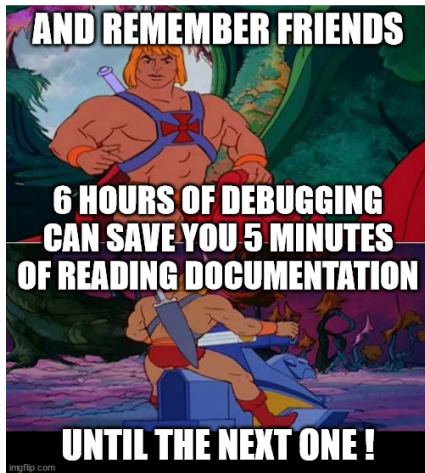
Naše problémy



imgflip.com



Naše problémy



Děkuji za pozornost

Adam Beneš & Jiří Antoňů • techsupport@mojeid.cz

