Úvod

Společnost E.ON využívá pro správu, autentizaci a autorizaci centrální Identity management, který slouží celé skupině E.ON. V rámci české republiky existuje lokální řešení, které je na centrální napojeno a přidává drobné funkcionality pro jednodušší správu a automatizaci. Implementátor aplikací se bude napojovat pouze na lokální řešení (aplikace SARA) a integrace na centrálu nemusí řešit.

 

SP – Service Provider, aplikace žádající o přihlášení, poskytuje koncové služby uživatelům.

IDP – Identity Provider, z pohledu SP aplikace poskytující identity a autentizaci/autorizaci.

Identifikace uživatele

Každý uživatel v rámci skupiny obdrží jedineční identifikátor zvaný **KID**, který seskládá z velkého počátečního písmene jména následovaný 4-5 číslicemi. Uživatelem je míněno interní zaměstnanec i partner vykonávající činnost pro člena skupiny na základě jakékoliv smlouvy. Identifikátory KID tedy neobdrží koncový zákazník E.ONu (maloodběratel/velkoodběratel).

**TABULKA 1: KATEGORIE UŽIVATELŮ**

|  |  |
| --- | --- |
| Kategorie uživatelů  | Identifikátor  |
| Zaměstnanci  | KID  |
| Partneři/dodavatelé  | KID  |
| Zákazníci  | XID  |

Autentizace

Autentizaci uživatelů zajišťuje komponenta Access Management realizovaná standardním řešením WSO2 Identity Server. Federativní přihlášení je možné realizovat pomocí dvou protokolů – OIDC (OpenId Connect) a SAML2.

OIDC

OIDC protokol je hojně využívaný sociálními službami (Facebook, Twitter, …) nebo poskytovateli veřejných služeb (Google, Amazon, Microsoft, …). Zakládá se na protokolu OAuth2, který vydává tzv. Access Token a přidává informace o uživateli pomocí JWT tokenu případně služby UserInfo. V rámci lokálního i centrálního řešení jsou podporované pouze 3 autentizační flow -  Client Credentials Grant, Authorization Code Grant a Authorization Code Grant with KPCE. Každé flow je použité pro speciální požadavky aplikace (SP), které jsou znázorněné na obrázku 1.

 **OBRÁZEK 1: POUŽITÍ OIDC FLOW**

Pro bližší popis je možné vycházet z <https://rograce.github.io/openid-connect-documentation/explore_auth_code_flow>.

 

**OBRÁZEK 2: OIDC AUTHORIZATION CODE FLOW**

SAML2

SAML2 je protokol na ústupu, nicméně je ve skupině stále použitelný pro autentizaci. V současné době používáme pouze flow HTTP Redirect Binding, které je použitelné pro webové aplikace, méně už pro nativní vůber pro autentizaci machine to machine. Základní schéma je na obrázku 3.

 

**OBRÁZEK 3: SAML2 HTTP REDIRECT BINDING**

Authorizace

Pro SP je nepovinnou možností využití centrálního modulu autorizace, v tomto případě poskytnutí uživatelských rolí. Zda tento modul bude použit zaleží na rozhodnutí projektu na základě požadavků. Autorizace je poskytována pouze v případě využití protokolu OIDC přes volání služby UserInfo, která vrací seznam uživatelských atributů.

Jinou možností je přímé napojení na Userstore aplikace SARA. User provisioning není podporován.

Postup napojení na SARA

1. Registrace aplikace v SARA
2. Kontaktování SARA týmu, komunikace ohledně kategorie uživatelů
3. výběr vhodného protokolu + výběr vhodného flow
4. Poskytnutí vstupních informací o aplikaci – primárně název a Callback URL
5. Implementace zvolené autentizační metody
6. SP obdrží identifikátory nutné pro implementaci protokolu od SARA týmu (URL, client\_id, client\_secret, consent\_url, …)
7. Založení uživatelských účtů v centrálním IDM
8. Vytvoření KID

Prostředí

Aplikace SARA sestává ze tři prostředí – vývojové, testovací a produkční. SP se zakládají na všech prostředích, mandatorní je využití minimálně prostředí testovací a produkční. Pro vývojové účely je možné vytvořit SP s calback URL směřující na localhost.

Ostatní

Referenční příručka:



Seznam klientských knihoven: <https://openid.net/developers/certified/>