IS4U

INTERNSHIP ASSIGNMENT

MAN-IN-THE-MIDDLE: OPENID CONNECT

Contact

Cindy Van den Hoecke
careers@is4u.be

IS4U NV

Veldkant 7
2550 Kontich
België

Omschrijving

Voor de verschillende access management oplossingen die door IS4U worden geïmplementeerd, is het vaak nodig de verschillende OAuth2 grants / OpenID Connect (OIDC) flows te troubleshooten en/of testen.

Om bepaalde issues te kunnen reproduceren is het dan nodig om bv. voor een bepaalde OIDC client/ flow een token met een specifieke scope etc. op te vragen, daar dan bepaalde acties mee uit te voeren (vb: refresh token, exchange token, revoke ...), om zo tot het gewenste resultaat te komen.

De bedoeling van deze stageopdracht is om een "test / debug tool" te ontwikkelen waarin je verschillende integratiescenario's kunt nabootsen.

Dit mag een web app zijn, een browser extension of een "desktop app", maar hou er wel rekening mee dat het nodig zal zijn om een http redirect of post naar een domeinnaam die niet in ons bezit is te kunnen onderscheppen (lokale app) of herschrijven/wijzigen naar een eigen domeinnaam (web app).

Voorbeeld van een use case:

Een OIDC access token ophalen voor een bepaalde client met een bepaalde user, gebruik makende van de "authorization code flow", de authorization code wordt teruggestuurd naar een bepaalde endpoint (een URL die niet wij niet beheren) met een 302 redirect waarin een "code" parameter zit.
De bedoeling is om de redirect response te onderscheppen, om daarna met een "client_id" en "client_secret" de authorization code om te wisselen voor tokens (access token, refresh token, id token).

Eens je deze tokens hebt, moet het mogelijk zijn om andere acties te triggeren: refresh token gebruiken om een nieuwe access token te verkrijgen, userinfo endpoint op de access manager aanspreken, token revoken, end_session endpoint gebruiken, naar een willekeurige url kunnen posten met de access token in een bearer header etc.

Minimale vereisten

De studenten wordt gevraagd minimaal de volgende functionaliteiten op te leveren:

- OIDC Discovery endpoint parsen om zo de verschillende endpoints op te halen
  - voorbeelden van OIDC discovery endpoints:
    - https://sso.redhat.com/auth/realms/redhat-external/.well-known/openid-configuration
    - https://accounts.google.com/.well-known/openid-configuration
- Manueel de endpoints kunnen ingeven in het geval er geen discovery endpoint beschikbaar is
- OAuth2 / OIDC grants / flows integreren:
  - authorization code flow
  - client credentials flow
- Client authentication methodes:
  - client_secret_basic
  - client_secret_post
- Scopes kunnen ingeven (https://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims)
- Tokens ophalen a.d.h.v. de geselecteerde flow
- Token kunnen refreshen (met "checkbox" optie om de refresh token wel of niet te vervangen)
- UserInfo endpoint oproepen met een access token
- Revocation endpoint
- Token introspection endpoint oproepen om de verschillende tokens te valideren
- Custom endpoint: url manueel kunnen ingeven, http method selecteren (GET / POST / PUT /DELETE), authentication method (bearer, basic, post ...)

- Tokens kunnen bekijken (zie https://jwt.io) om de payload (claims) na te kijken en te valideren

Optioneel:

- OIDC client authentication methodes: client_secret_jwt, private_key_jwt
- Clients kunnen bewaren (encrypted en importable / exportable)
- Templates van endpoints kunnen bewaren en hergebruiken (zie custom endpoint onder "vereisten")
    - Dit zou dan bijvoorbeeld kunnen gebruikt worden om een Keycloak specifieke endpoint te voorzien zoals "Revoke consent and offline tokens for particular client from user", zie https://www.keycloak.org/docs-api/4.8/rest-api/index.html
- Placeholders kunnen gebruiken in (templates van) custom endpoints, vb: {TOKEN_ENDPOINT} of {ACCESS_TOKEN:sub} of {ID_TOKEN:azp} etc.
- ·Custom requested claims kunnen ingeven (https://openid.net/specs/openid-connect-core-1_0.html#ClaimsParameter)
- PKCE support (Proof Key for Code Exchange) voor OAuth2 / OpenID Connect
- PAR support (Pushed Authorization Requests) - https://datatracker.ietf.org/doc/html/rfc9126
- JARM support (JWT-Secured Authorization Response Modes) - https://openid.net/specs/oauth-v2-jarm.html

Projectmethodologie

IS4U maakt voor haar projecten gebruik van agile projectmethodologieën zoals XP en SCRUM. Het hierboven beschreven project vormt hier geen uitzondering op. Deze methodologieën stellen de kwaliteit van software oplossingen centraal. Dit wordt bereikt door het project op te delen in kortere iteraties en een zeer intense communicatie binnen en buiten het project team. Intensieve communicatie is inherent aan agile en leidt bijgevolg tot een doorgedreven stagebegeleiding.