Opgave: Open Authentication

Versiegeschiedenis

- 13/01/2021: initiële versie

Doelstellingen

Na deze opgave moet je:

- Het verschil kunnen uitleggen tussen authenticatie via een eigen 'proprietary' mechanisme en een externe authenticatie-service.
- Volgende termen/begrippen kunnen uitleggen: OAuth, OpenID Connect, Google Identity, Facebook connect, Microsoft Identity, Access Token, Bearer Token, Refresh Token, JWT
- De authenticatie voor een eigen toepassing (web-App, Web-API en/of stand-alone/mobile toepassing) kunnen realiseren via een externe authenticatie-service.

Opgave

Inleiding

In heel wat toepassingen moet je de identiteit van de gebruiker kennen. Daar kunnen een aantal redenen voor zijn:

- ➔ Authorisatie: om te bepalen wat de rechten zijn van een gebruiker is het uiteraard essentieel dat je zijn/haar identiteit met zekerheid kent.
- ➔ Voor het bijhouden van gebruikersafhankelijke informatie en het persisteren daarvan over verschillende sessies (bv. het bijhouden van een gebruikersprofiel).
- ➔ Voor het koppelen van de identiteit van een gebruiker tussen verschillende toepassingen.

Uiteraard kan je zelf een authenticatiemechanisme uitwerken door bv. een gebruikersnaam en (salted) hash van het paswoord op te slaan in een databank.
Die werkwijze heeft echter een aantal nadelen:

- ➔ Je moet zelf instaan voor een degelijke, veilige implementatie waarbij ook de authenticatiegegevens in de databank afdoende beveiligd moeten worden.
- ➔ Je moet de nodige voorzieningen (en code) hebben voor het aanpassen/resetten van paswoorden op een veilige manier.
- ➔ Je gebruikers moeten specifiek voor jouw toepassing een afzonderlijke gebruikersnaam en paswoord onthouden en erop vertrouwen dat jouw toepassing daar voldoende veilig mee omgaat.
- ➔ Op deze manier is het zeer moeilijk om een 'single sign on' oplossing te realiseren tussen verschillende toepassingen (zeker als je die niet allemaal zelf beheert).

➔ Het gebruik van een (veiligere) multi-factor authenticatie kan erg complex zijn en vraagt extra infrastructuur.

Om die redenen zijn er een aantal initiatieven en standaarden ontstaan voor het authenticeren van gebruikers via externe authentication services (zeker na te kijken: OAuth 2.0, OpenID Connect).

In praktijk zijn er een aantal grote spelers uit sociale media die hun eigen authenticatie-systeem beschikbaar stellen voor authenticatie in '3rd party' toepassingen via open standaarden of varianten daarop: Google, Facebook, Microsoft…

Opgave

- Zoek informatie op over volgende termen en begrippen: OAuth, OpenID Connect, Access Token, Bearer Token, Refresh Token, JWT
- Zoek inleidende informatie op over hoe de grote spelers (Google, Facebook, Microsoft) externe authenticatie-services aanbieden en hoe je daar vanuit je eigen toepassing gebruik van **zou** kunnen maken.
- Schrijf zelf een 'proof of concept' toepassing (WebApp, WebApi, Mobile App, desktoptoepassing of combinatie daarvan) waarbij je authenticatie realiseert via een externe authentication service.
  Tip: ook onze opleiding heeft infrastructuur voor externe authenticatie via OpenID Connect (met je schoolaccount). Als je die wilt gebruiken, neem je contact op met tom.cordemans@odisee.be).

  Vereisten:
  - Een deel van je toepassing moet publiek toegankelijk zijn (bv. een homepage).
  - Aanmelden moet mogelijk zijn. Daarbij mag uitsluitend gebruik gemaakt worden van een externe authentication-service.
  - Je toepassing moet na het inloggen aan de gebruiker tonen welke persoonlijke informatie er via de authenticatie-service over hem/haar beschikbaar is.
  - Je toepassing moet (zelf te kiezen) individuele informatie (niet afkomstig van de authenticatie-service) van een gebruiker bijhouden en die weergeven wanneer de gebruiker ingelogd is.

- Zorg voor de nodige documentatie zoals opgelijst bij 'Deliverables'.

Deliverables

- een korte uitleg van volgende termen: OAuth, OpenID Connect, Access Token, Bearer Token, Refresh Token, JWT en een beschrijving van de context waarin ze gebruikt worden
- een kort overzicht van de mogelijkheden voor externe authenticatie via minimaal Google, Facebook, Microsoft
- je werkende 'proof of concept' toepassing en de sources daarvan
- een logboek waarin je bijhoudt hoe je tewerk gegaan bent,welke problemen je ondervond en hoe je ze opgeloste.
- een korte technische beschrijving van je toepassing

- een demonstratiefilmpje (op youtube) met link in je documentatie. Daarin toon je de werking van je toepassing met authenticatie

Opmerking: De verschillende tekstdocumenten (uitleg, overzicht, logboek, technische beschrijving) mogen eventueel samengevoegd worden tot één document.