

Kravspesifikasjon SSO autentisering mot Entra ID - Møre og Romsdal fylkeskommune

Hovedkrav

- All filtrering av brukerdata og tilgangsstyring skal defineres av Oppdragsgiver i Entra ID.
- Tilgangsstyring gjøres ved at Oppdragsgiver tildeler enkeltpersoner eller grupper tilgang til definert Enterprise Application for SSO i Oppdragsgivers Entra ID *tenant* (leier).
- Innlogging og overføring av brukerdata til leverandørs løsning skal kun være tilgjengelig for brukere som har blitt gitt eksplisitt tilgang til definert Enterprise Application for SSO i Oppdragsgivers Entra ID *tenant* (leier).
- Det gis aldri tilgang til Microsoft Graph API mot Oppdragsgivers Entra ID *tenant* (leier) som ikke er filtrert på Oppdragsgivers side med filtrering som Oppdragsgiver kontrollerer.

Scenario: Basic authentication

Ment for applikasjoner som kun trenger autorisasjon for brukerinlogging, og ikke lagrer brukerdata eller lagrer minimalt med brukerdata slik som navn, UPN, og epostadresse.

Dersom bruker eller grupper av brukere hos Oppdragsgiver skal ha spesielle tillatelser eller tilganger i leverandørs løsning som avviker fra andre brukere hos Oppdragsgiver som også har tilgang til løsningen, eller det er behov for flere detaljer fra brukerobjekter enn tillatelsene listet under gir, eller det er behov for bruker- og/eller gruppeprovisjonering fra Oppdragsgiver til leverandørs løsning, skal dette scenarioet *ikke* brukes.

En brukers gruppemedlemskaper skal ikke overføres i dette scenarioet.

Kan settes opp/defineres enten av leverandør eller av Oppdragsgiver.

- Definert av leverandør
 - Leverandør oppretter applikasjon i sin egen *tenant* (leier) eller løsning, og gir Oppdragsgiver en URL som Global Admin benytter for å godkjenne tilgang på vegne av organisasjonen.
- Definert av Oppdragsgiver
 - Leverandør gir Oppdragsgiver nødvendige detaljer for oppsett av applikasjon i Oppdragsgivers Entra ID *tenant* (leier).

For begge gjelder følgende:

- Må bruke Microsoft identity platform (Azure AD/Entra ID) v2.0 endpoint for authentication
- Må bruke Open ID Connect (OIDC) protokoll
- Applikasjonen kan kun ha [Delegated access](#) med Admin consent på vegne av organisasjonen til *påloggende brukers profil*, bestående av en eller flere av tillatelsene:
 - Sign users in (openid) ([Microsoft documentation](#))
 - View users' basic profile (profile) ([Microsoft documentation](#))
 - View users' email address (email) ([Microsoft documentation](#))
 - Maintain access to data (...) (offline_access) ([Microsoft documentation](#))Merk at med *offline_access* skal data lagret hos leverandør automatisk slettes innen 30 dager fra bruker ikke lenger har tilgang til SSO-app.
 - **User.read** skal ikke brukes. Om det trengs tilgang til Graph API, skal dette scenarioet *ikke* brukes.
- Oppdragsgiver praktiserer *Principle of Least Privilege*, så tillatelser og claims skal kun inneholde et minimum av nødvendige scope og felt som trengs for leverandørs løsning.

Scenario: SAML 2.0

Ment for applikasjoner der brukere skal ha profil, tilganger og/eller data spesifikt for hver bruker, eller en gruppe brukere, i leverandørs løsning.

Skal følge [SAML 2.0-standarden](#), tilpasset Oppdragsgivers autentiseringsløsning.

Settes opp av Oppdragsgiver i Oppdragsgivers autentiseringsløsning. Per tiden er dette Entra ID, men leverandørs løsning må støtte at Oppdragsgiver skifter autentiseringsløsning med minimale konfigurasjonsendringer i leverandørs løsning.

Om det er behov for brukerprovisjonering, skal det benyttes SCIM (se eget punkt). Oppdragsgiver bestemmer om SCIM settes opp som funksjon av SSO-applikasjon eller frittstående i samme eller et annet system.

Alle data assosiert med en spesifikk bruker skal, dersom SCIM ikke benyttes, slettes automatisk senest 30 dager etter bruker ikke lenger har tilgang til SSO-applikasjonen.

Leverandør gir Oppdragsgiver detaljer som behøves for å sette opp SSO-applikasjon. Dette inkluderer mellom annet:

- **Identifier** (Entity ID)
- **Reply URL** for leverandørs løsning
- Eventuell **Sign on URL** for leverandørs løsning
- Eventuell **Logout URL** for leverandørs løsning
- Hvilke Attributes og Claims som trengs som minimum. Oppdragsgiver praktiserer *Principle of Least Privilege*, så claims skal kun inneholde et minimum av nødvendige felt.

Oppdragsgiver vil så gi leverandør SAML Certificate gjennom en på forhånd avtalt sikret forbindelse, samt Metadata Url, Login URL, Identifier URL, og eventuelt Logout URL.

Scenario: OIDC/OAuth 2.0

Ment for applikasjoner der brukere skal ha profil, tilganger og/eller data spesifikt for hver bruker, eller en gruppe brukere, i leverandørs løsning, hvis SAML ikke er mulig.

Benytter [Open ID Connect standarden](#), tilpasset Oppdragsgivers autentiseringsløsning.

Settes opp av Oppdragsgiver i Oppdragsgivers autentiseringsløsning. Per tiden er dette Entra ID, men leverandørs løsning må støtte at Oppdragsgiver skifter autentiseringsløsning med minimale konfigurasjonsendringer i leverandørs løsning.

Om det er behov for brukerprovisjonering, skal det benyttes SCIM (se eget punkt). Oppdragsgiver bestemmer om SCIM settes opp som funksjon av SSO-applikasjon eller frittstående i samme eller et annet system.

Alle data assosiert med en spesifikk bruker skal, dersom SCIM ikke benyttes, slettes automatisk senest 30 dager etter bruker ikke lenger har tilgang til SSO-applikasjonen.

Leverandør gir Oppdragsgiver detaljer som behøves for å sette opp SSO-applikasjon. Merk at Oppdragsgiver praktiserer *Principle of Least Privilege*, så claims skal kun inneholde et minimum av nødvendige felt.

Roller

Dersom leverandørs applikasjon har mulighet for å tildele ulike roller for Oppdragsgivers brukere, slik som for definerte tilganger, skal dette defineres som AppRole ([Microsoft documentation](#)) som blir overført som del av *token* under innlogging.

Leverandør definerer AppRole med navn og Value og gir liste med dette til Oppdragsgiver. Oppdragsgiver tildeler brukere/grupper rolle i Enterprise Application. Leverandør definerer så mapping i sin løsning for hver AppRole.

Alternativt oppretter Oppdragsgiver sikkerhetsgrupper som skal mappes mot hver rolle internt i leverandør løsning.

Oppdragsgiver gir leverandør liste over navn/ObjectID, og leverandør mapper hver gruppe mot ønsket rolle. Alternativt gir leverandør tilgang til at Oppdragsgiver selv kan sette slik mapping inne i løsningen.

Ved bruk av Group Claims for å se hvilke grupper påloggende bruker er medlem i, skal kun detaljer for grupper assosiert med/tildelt SSO-applikasjonen returneres i claim. Øvrige grupper brukere er medlem i, skal ikke returneres. Om slik begrensning ikke er mulig å sette opp i Oppdragsgivers autentiseringsløsning, eller det trengs provisjonering eller flere detaljer om gruppene, skal det benyttes SCIM provisjonering av grupper (se eget punkt om SCIM), og Group Claims skal ikke brukes.

SCIM 2.0

System for Cross-domain Identity Management. Benyttes når det behøves brukerprovisjonering i leverandørs løsning.

Skal følge SCIM 2.0-standard.

Se [Understand the Microsoft Entra SCIM Implementation](#) for detaljer om minimumskrav når det gjelder Microsoft Entra ID, som benyttes av Oppdragsgiver som IdP per dato.

Se <https://scim.cloud> for definisjoner og mer informasjon om protokollstandarden.

Leverandørs løsning skal fungere som *Server* under SCIM-standard og skal ha tilhørende SCIM-API (endepunkt), og må støtte at Oppdragsgiver endrer kildesystem (IdP) med minimale konfigurasjonsendringer i leverandørs løsning. Leverandørs SCIM-API for tilbudt løsning må som minimum støtte *Create, Read, Update og Delete (CRUD-operations)* av brukerobjekter og eventuelt gruppeobjekter, initiert av Oppdragsgivers *Client* (IdP). Oppdragsgivers *Client* (IdP) kan ha krav utover dette, som leverandørs løsning må støtte.

Leverandørs Server må gi tilbakemeldinger etter SCIM-standard til oppdragsgivers Client for operasjoner, slik at oppdragsgivers Client får korrekte logger for operasjoner slik som dersom en brukerkonto eller gruppe allerede finnes.

Leverandørs løsning må logge operasjoner utført av SCIM-synk og bør gjøre disse loggene enkelt tilgjengelig for oppdragsgivers brukere med adminrolle i løsningen eller brukere med egen rolle for lesing av slik logg. Loggen må inneholde tydelig liste over hvilke kontoer eller grupper som er forsøkt utført operasjoner for, og resultatet av hver operasjon. Dette slik at leverandør og/eller oppdragsgivers adminbruker eller loggleser kan benytte loggen i feilsøking.

Ved SCIM *Delete*, skal data assosiert med bruker øyeblikkelig slettes i leverandør systemer, det skal ikke benyttes «papirkurv»/«soft delete». Unntak er data nødvendig for løsningens funksjon, og skal da godkjennes av Oppdragsgiver.

Oppdragsgiver bestemmer om SCIM settes opp som funksjon av SSO-applikasjon eller frittstående i samme eller et annet system.

Leverandør gir Oppdragsgiver detaljer for oppsett:

- *Tenant URL* for leverandørs SCIM-API og tilhørende *Secret Token* assosiert med Oppdragsgiver.
- Hvilke *Attribute Mappings* som er nødvendig som minimum, både for brukere og eventuelt sikkerhetsgrupper hvis disse skal benyttes i leverandørs løsning.