Digdir

digdir.no

OIDC/OAuth2-autentisering i Altinn REST API

Litt historikk

- Altinn har siden 2003 tilbudt API-er for sluttbrukere og virksomheter i Altinn
- Både SOAP (WCF) og REST tilbys som kanaler i dag
- >200 millioner kall per måned
- Autentiseringsmekanismer (før 20.11)
  - Brukernavn/passord (systemid/passord)
  - PIN-kode på SMS (kun SOAP)
  - Cookie-basert (kan kombineres med ID-porten)
  - Virksomhetssertifikat – kan også kombineres med virksomhetsbrukere

Problemer med autentiseringsmekanismene

- Hemmelighetsbasert – man må oppgi brukernavn/passord til en tredjepart
- SMS-pin gir lavt sikkerhetsnivå
- Cookie-basert autentisering krever «hijacking» av cookielager i tykke sluttbrukerapplikasjoner
- For eksterne portaler må integrasjonen gjøres på klientsiden
- Browser-støtte for tredjepartscookies på tur ut

Løsningen – OIDC/OAuth2

- Unngår deling av hemmeligheter til tredjeparter
- Bedre kontroll over hvordan systemer bruker egen tilgang
- Mer finkornet tilgangsstyring
- Høyere sikkerhetsnivå
- Mulighet for portalintegrasjoner i backend, uten bruk av cookies
- Maskinporten som erstatning for virksomhetssertifikat

ID-porten + Maskinporten + Altinn = sant

- Personinnlogging implementert i 20.11-release av Altinn
  - Maskinporten-støtte fra 20.7
- Krever eksplisitt autorisasjon fra bruker
- Kommer samtidig med et par nye features i ID-porten
- Vil i kommende release kunne administrere autoriserte apper og nettsteder direkte fra Altinn

Demonstrasjon

digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarevegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo