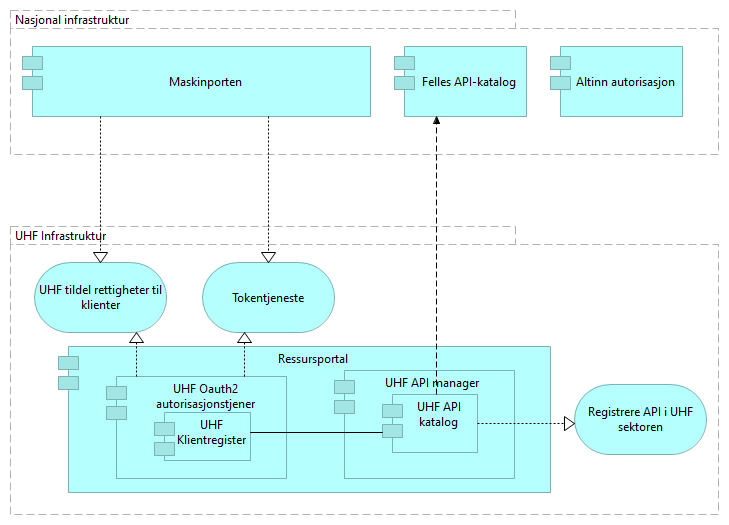
API management integrert med nasjonale felleskomponenter

2021-02-16

​​Det er behov for datadeling og API Management på tvers av sektorer. Høyere utdanning og forskning ønsker utstrakt bruk av nasjonale felleskomponenter, som omtalt i Digitaliseringsrundskrivet. For å oppnå dette må både sektorens og den nasjonale infrastrukturen videreutvikles.​

Føderert tilgangsstyring for datadeling på tvers av sektorer er ønskelig, og det krever blant annet standardisering av tilgangstokens for å oppnå gjennomgående tillitskjeder. ​Det er også ønskelig at brukere kan styre samtykke til sine data fra et sted nasjonalt, inklusivt til data i kilder i høyere utdanning og forskning. Det hadde vært ønskelig om en felles Norsk samtykketjeneste kunne være integrert med funksjonalitet som vi forvente skal realiseres i IAM løsningent til høyere utdanning og forskning.

Figuren viser kun kobling til maskinporten direkte som er mulig i dag. Det er planlagt automatisert høsting av API katalogen fra høyere utdanning og forskning til Felles API-katalog som visst i figuren. Samtykke til kilder i vår sektor fra Altinn autorisasjon er foreløpig ikke imlementert, så ingen kobling til Altinn autorisasjon er visst i figuren. ​



API management integrert med nasjonale felleskomponenter

Elementer i view for API management integrert med nasjonale felleskomponenter

|  |  |
| --- | --- |
| Element | Beskrivelse |
| UHF Infrastruktur <grouping> | Felleskomponenter i UHF-infrastrukturen for datadeling |
| Tokentjeneste <application-service> | Tjeneste som utsteder sikkerhetsbilletter. Sikkerhetsbillett utstedes basert på tildelte rettigheter og eventuelle representasjonsforhold. |
| Registrere API i UHF sektoren <application-service> | Programtjeneste for å registrere og vedlikeholde API som er tilgjengelige i Universitets og Høyskole-sektoren |
| UHF tildel rettigheter til klienter <application-service> | Tildel autoriserte rettigheter basert på roller, annen policy eller manuel behandling av dataforvalter gjennom tjenesten "Forespør dataforvalter". |
| Ressursportal <application-component> | Ressursportalen holder oversik over og tildeler tilganger til beskyttede ressurser i høyere utdanning og forskningssektoren i henhold til føringer fra eierne av disse ressursene. Tilganger er gitt i form av OAuth2 grants og tokens. Ressursportalen er en del av den felles infrastrukturen for føderert API management for høyere utdanning og forskning. Den registrerer og holder oversikt over API, holder oversikt over klienter som har blitt tildelt tilgang til API og hvilke tilganger det gjelder. Ressursportalen benytter Jason Web Token formattert OAuth2 sikkerhetstoken for å gi tilgang til ressurser gjennom API gateway nær de beskyttede ressursene. |
| UHF Oauth2 autorisasjonstjener <application-component> | Autorisasjonstjenester realiserer tilgangskontroll gjennom å utstede OAuth 2 grants og tokens. En autorisasjonstjener er også brukt til å realisere tilgangs policy. |
| UHF Klientregister <application-component> | Oversikt over alle klienter som er blitt tildelt tilgang til ressurser. |
| UHF API manager <application-component> | Administrativ komponent som kontrollerer policy og livssyklus for definisjon og forvaltning av API. Tilganger gjennom et API defineres i API manager og tildeles av autorisasjonstjener.  Ansvaret til API manager inkluderer: \* Sentralisert API Gateway som håndterer sikkerhetsretningslinjer, og sender kall til bakenforliggende API \* Sentralisert publisering av API spesifikasjon (OpenAPI/RAML), dokumentasjon \* Sentralisert API administrasjon og forvaltning av API-katalogen \* Håndtering av registrerings- og introduksjonsprosesser for API utviklere \* Håndtere livssyklusen til et API, uvikling, test, utrulling, nye versjoner, nedlegging \* Ivareta registrering, forvaltning og og utvikling av klientrettigheter \* Rapportering og analyse for å monitorere bruk og last |
| UHF API katalog <application-component> | Oversikt over alle API som er registrert  UHF API katalog kan inneholde \* Navn på API \* Tekstlig beskrivelse av API \* Informasjonsmodell / Datamodell for API som tilbys \* Kildeinformasjon for data, begrepsinformasjon \* Informasjon om tilgang, juridiske og tekniske begrensinger for bruk \* Eksempelkode, interaktiv API-konsoll og sandkasse for test \* Informasjon om hvordan få support og hjelp fra utsteder |
| Nasjonal infrastruktur <grouping> | Nasjonale felleskomponenter for datadeling |
| Maskinporten <application-component> | [Torget] Maskinporten er en løsning for tilgangsstyring for virksomheter som utveksler data. Løsningen garanterer identiteten mellom virksomheter, og sørger for maskin-til-maskin autentisering.  [Verktøykasse for deling av data] Maskinporten sørger for sikker autentisering og tilgangskontroll for datautveksling mellom virksomheter, maskin til maskin. Dette gir teknisk og organisatorisk samhandlingsevne.  Mer om Maskinporten: <https://www.digdir.no/digitale-felleslosninger/maskinporten/869> |
| Altinn autorisasjon <application-component> | [Torget] Autorisasjonskomponenten i Altinn som gir muligheter til å delegere rettigheter til andre organisasjoner eller personer. Rettigheter til bruk av autorisasjonskomponenten baserer seg på registrerte roller i Enhetsregisteret. Altinn autorisasjon leverer også tjenester for å registrere og kontrollere samtykke gitt av person eller virksomhet.  [Verktøykasse for deling av data] Altinn autorisasjon gir teknisk samhandlingsevne ved at bruker logger inn med elektronisk ID, autorisasjonskomponenten sjekker at bruker har de tilgangene som kreves for å ta i bruk aktuell tjeneste.  Dersom en privatperson skal ta i bruk en tjeneste på vegne av en virksomhet, gjøres det et oppslag mot Enhetsregisteret for å bekrefte at personen har en rolle på vegne av virksomheten. Dette gir organisatorisk samhandlingsevne.  Mer om Altinn autorisasjon: <https://www.altinndigital.no/produkter/styring-av-tilgang/> |
| Felles API-katalog <application-component> | Del av Felles datakatalog som gir mulighet for å søke etter API-er og lese API-spesifikasjoner <https://fellesdatakatalog.brreg.no/apis> |