Føderert API management

2021-02-16

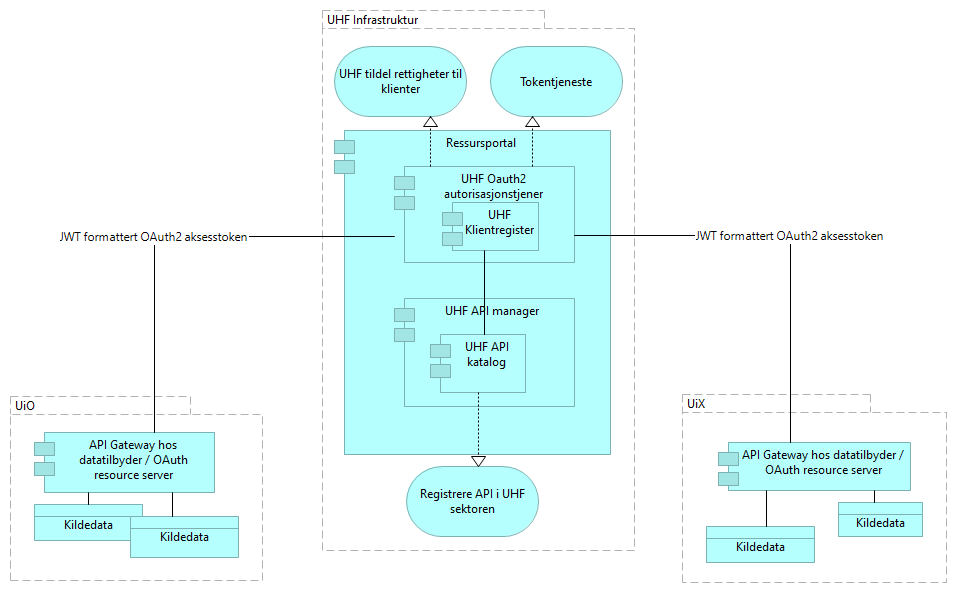
Føderert API Management innebærer at et domene (føderasjon) kan gi brukere i andre domener man har et tillitsforhold til (ofte kalt fødereringspartnere) tilgang til sine egne data gjennom APIer. Dette er et prinsipp for API Management som har etablert seg de siste årene. Det er flere grunner for dette, blant annet at store virksomheter i dag gjerne har virksomhetsdata lagret distribuert og gjerne fordelt mellom systemer som kjører på lokale servere (on-premise) og i skybaserte-løsninger som kjører på egen infrastruktur.

Det sterke politiske fokuset på deling av data gjennom orden i eget hus og nasjonale og sektorvise digitaliseringsstrategier understøtter også behovet for et API Management regime som understøtter deling av data til 3. part for innovasjon, og fokus på sammenhengende brukerreiser (eksemplifisert ved de syv livshendelser og tjenestekjeder) som forutsetter at data kan deles mellom virksomheter som betjener slike brukerreiser.

Virksomhetene i UH/F har mange fellestrekk og noen fellestjenester på tvers, men deres autonomi gjør at de også er ulike på enkelte områder, f.eks. når det gjelder teknisk infrastruktur. Dette understreker behovet for en føderert API Management løsning som er mer fleksibel mtp. tekniske løsninger og produktvalg lokalt.

Designen avbildet er laget for å støtte følgende karakteristikk:

* Intstitusjonene er sikret råderett over egne data gjennom tilgangstjeneste i resssursportalen og API gateway hos institusjonen som kan styre og holde oversikt over datatilgang
* Institusjonene har valgfrihet over API Gateway såfremt funksjoner og grensesnitt er ivaretatt
* Deling av data på tvers av institusjoner er støttet gjennom felles ressursportal



Føderert API management

Elementer i view for Føderert API management

|  |  |
| --- | --- |
| 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. |
| 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 |
| 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". |
| UiX <grouping> |  |
| Kildedata <data-object> | Dataprodukt som tilbys av datatilbyder Produktet kan være fra en kilde eller sammensatt av flere innen et domene |
| API Gateway hos datatilbyder / OAuth resource server <application-component> | API gateway beskytter ressurser og monitorerer tilgang. Den håndhever tilgangsstyring ved å validere aksesstokens og utfører eventuell fin-granulert tilgangskontroll. Den håndhever også volumbegrenseninger og samler data om bruken av APIer (logging).  Komponent som beskytter ressursene og monitorerer tilgang inklusivt:  \* Validere tilgangstoken \* Beskytte mot inntrenging og andre trusler \* Håndtere volumbegrensninger og andre abonnementsordninger \* Håndheve tilgangsstyring \* Samle inn data om bruken av API-er \* Orkestrering mellom interntjenester |
| Kildedata <data-object> | Dataprodukt som tilbys av datatilbyder Produktet kan være fra en kilde eller sammensatt av flere innen et domene |
| UiO <grouping> |  |
| Kildedata <data-object> | Dataprodukt som tilbys av datatilbyder Produktet kan være fra en kilde eller sammensatt av flere innen et domene |
| API Gateway hos datatilbyder / OAuth resource server <application-component> | API gateway beskytter ressurser og monitorerer tilgang. Den håndhever tilgangsstyring ved å validere aksesstokens og utfører eventuell fin-granulert tilgangskontroll. Den håndhever også volumbegrenseninger og samler data om bruken av APIer (logging).  Komponent som beskytter ressursene og monitorerer tilgang inklusivt:  \* Validere tilgangstoken \* Beskytte mot inntrenging og andre trusler \* Håndtere volumbegrensninger og andre abonnementsordninger \* Håndheve tilgangsstyring \* Samle inn data om bruken av API-er \* Orkestrering mellom interntjenester |
| Kildedata <data-object> | Dataprodukt som tilbys av datatilbyder Produktet kan være fra en kilde eller sammensatt av flere innen et domene |