API management integrert med IAM

2021-02-17

Infrastruktur for identitetshåndtering og tilgangsstyring (IAM) utfyller API management og må fungere sammen.

Autentisering er det som sjekker at brukeren er kjent for virksomhenten og forsikrer at brukeren er den vedkommende gir seg ut for å være når brukeren ber om tilgang til ressurser.

Autorisering identifiserer hvilke tilganger en bruker skal ha til virksomhetens ressurser. Autorisasjon kan tildeles roller. Brukere kan tildeles roller og gjennom dette få autorisasjon til virksomhetens ressurser som er knyttet til rollen.

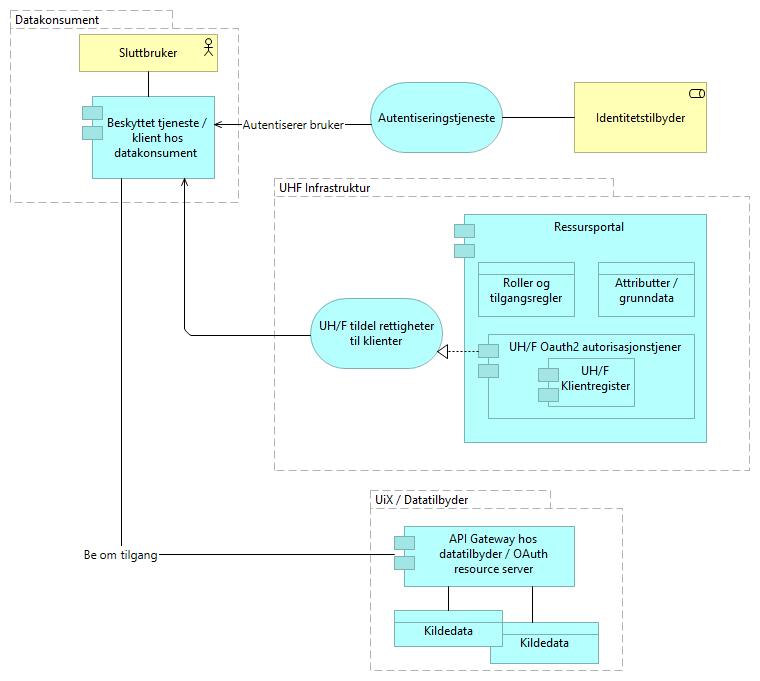
IAM utfører autentisering ved bruk av komponenter i den øvre delen av viewet.

API management utføres av komponenter i den nedre delen av viewet.

Ressursportalen og tjenesten for tildeling av rettigheter til klienter deltar i begge funksjoner.

IAM autoriserer sluttbrukeres tilgang til tjenester. Dette er basert på både autentisering av deres identitet, det vil si hvem brukeren er, og de roller brukeren er tildelt hos en eller flere institusjoner.

API management styrer tilgang til data gjennom API basert på policy eller godkjenning fra dataforvalter. Brukers tilgang til beskyttet tjeneste hos datakonsument kan være tilstrekkelig til at bruker ikke trenger å autoriseres eksplisitt hos datatilbyder. Avgjørelsen om å godkjenne tilgang til data kan godt være basert på en sluttbrukers rolle hos en institusjon. ​



API management integrert med IAM

Elementer i view for API management integrert med IAM

|  |  |
| --- | --- |
| Element | Beskrivelse |
| Datakonsument <grouping> | Komponenter som utgjør datakonsument, det vil si Universitetet, Høyskolens eller andre, sitt grensesnitt for datadeling |
| Sluttbruker <business-actor> | Personen som skal tildeles tilgang til beskyttede ressurser basert på identitet, roller og annen kontekst. |
| Beskyttet tjeneste / klient hos datakonsument <application-component> | Tjeneste som IAM beskytter tilgang til. Tjenesten kan også være en konsument av data gjennom API, det vil si Universitet, Høyskole eller andre som gir tilgang til data fra datatilbyder.  Komponenten tilbyr: \* autentisering gjennom en Autentiseringstjeneste \* oppslag i felleskomponeneter for tilgang til datatilbyders dataprodukter \* tilgang til ressurser hos datatilbyder |
| Identitetstilbyder <business-role> | En identitetstilbyder er en virksomhet som er godkjent til å utstede elektroniske identiteter for entydig identifikasjon av en fysisk person på et gitt sikkerhetsnivå. |
| UHF Infrastruktur <grouping> | Felleskomponenter i UHF-infrastrukturen for datadeling |
| Ressursportal <application-component> | Ressursportalen holder oversikt 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. |
| Roller og tilgangsregler <data-object> | Definisjon av roller som blir brukt til å styre autorisasjon for å gi tilgang for en klient til et eller flere API. Definisjon av regler for tilgang til et eller flere API |
| Attributter / grunndata <data-object> | Opplysninger om personer som skal benyttes i tilgangsstyring. |
| UH/F 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. |
| UH/F Klientregister <application-component> | Oversikt over alle klienter som er blitt tildelt tilgang til ressurser. |
| UH/F tildel rettigheter til klienter <application-service> | Tildel autoriserte rettigheter basert på roller, annen policy eller manuell behandling av dataforvalter gjennom tjenesten "Forespør dataforvalter". Om klienten er fra UH/F sektoren blir tildelt rettighetene lagret i UH/F klientregisteret i Ressusportalen. Om klienten er fra utenfor UH/F sektoren må tildelte rettighetene lagres et sted der Maskinporten har oversikten. |
| UiX / Datatilbyder <grouping> | Komponenter som utgjør datatilbyder, det vil si Universitetet eller Høyskolens, grensesnitt for datadeling |
| Kildedata <data-object> | Dataprodukt som tilbys av datatilbyder Produktet kan være fra en kilde eller sammensatt av flere innen et domene |
| 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 |
| Autentiseringstjeneste <application-service> | Tjeneste som benyttes av tilbyder for å autentisere aktuell konsument. |