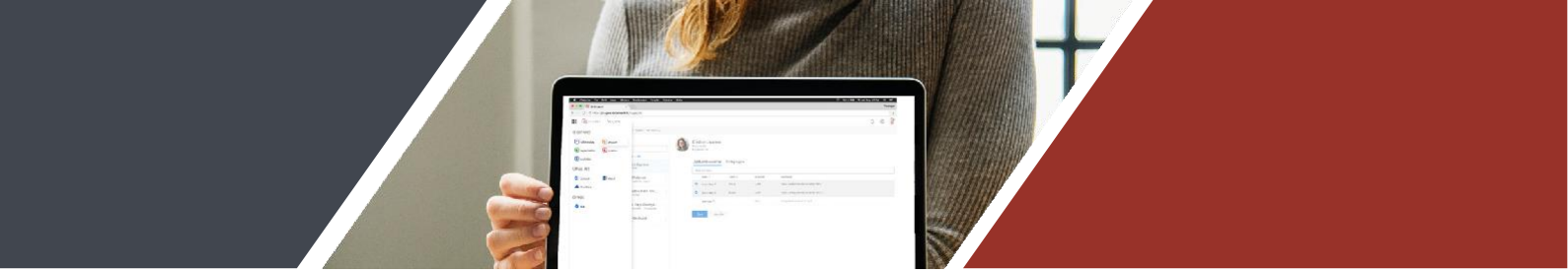


ID Connect: Sikkerhed og compliance

Dokument målrettet CISO, DPO og andre med interesse for informationssikkerhed.

Med en service fra ID Connect sikrer løsningen at hændelser til og fra eksterne services logges centralt, således at der er dokumentation og indsigt i adgangs- og rettighedsstyring på tværs af services.

ID Connect sikrer at kommunerne kan leve op til kravene omkring GDPR set i forhold til indsigt over hvem som har adgang til systemer og data og hvornår adgangen sidst har været benyttet. Det bliver også muligt at se hvilken leder der har godkendt medarbejderens adgang til de pågældende informationer.

Når log informationer centraliseres, er det samtidig muligt at anmode om sletning eller anonymisering af logdata, men alligevel fastholde anonymiserede data til statistik og historisk rapportering.

ID Connect tilbyder en vigtig platform, der kan hjælpe kommunerne med at omfavne den digitale omstilling på tværs af nye og gamle systemer.

Det gælder både indenfor bruger- og rettighedsstyring, men også indenfor adgang mellem de API- og servicelag der er nødvendige for at integrere nye og gamle services med hinanden.

Platformen medvirker til, at kommunen kan leve op til kravene fra f.eks. GDPR, samtidig med at de fordele der følger med GDPR i forhold til at understøtte det større lederansvar for informationer, udnyttes optimalt.

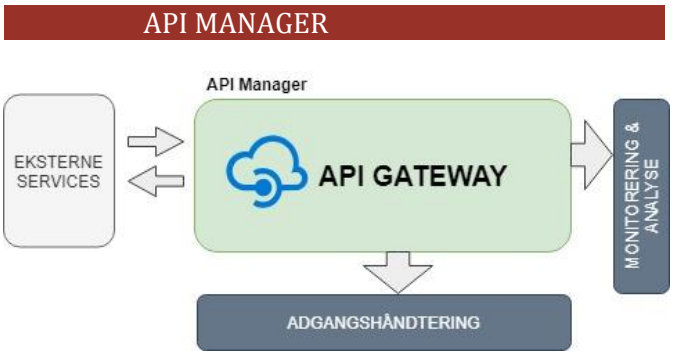
Vores platform er designet til at give sikker adgang på tværs af både nye og gamle systemer. Løsningen kan leve op til kravene om fuld indsigt herunder logning, men også sletning eller anonymisering af logs.

GDPR og informationssikkerhed

Fordi der i stort omfang er behov for at kunne behandle personoplysninger i kommunerne, er det vigtigt at have styr på databeskyttelsesforordningens krav til behandlingssikkerhed, hvem har adgang til data og hvilke hændelser der foretages på disse.

Løsningen kan reducere angrebsfladen, ved at begrænse adgangen til informationer ved hjælp af rollebaseret adgangsstyring, samtidigt med at den logger de hændelser, som er foretaget i ID Connect.

For at det kan lade sig gøre, og at datagrundlaget kan gøres tilgængeligt på en let tilgængelig måde, kanaliseres alle ændringer af data gennem en såkaldt API manager, der samtidig også håndterer en sikker godkendelse mellem servicelagene.

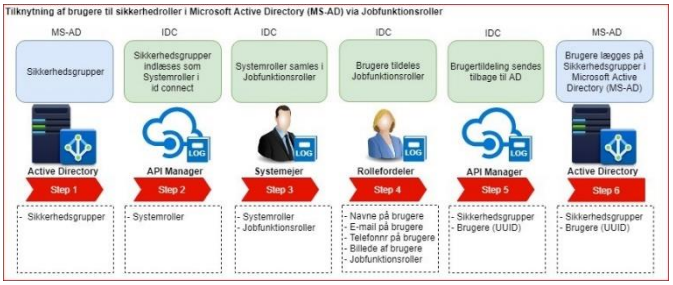


API manageren sikrer forbindelse mellem ID Connect og de services kommunen integrerer op mod. Alle hændelser på eksterne services logges og gøres tilgængeligt via en moderne analytics platform.

Derved inkluderer løsningen effektiv logning, analyse, men også monitorering og oversigt over alle hændelser.

Microsoft Active Directory (MS-AD)
Sikkerhedsgrupper og politikker

Med ID Connect får man mulighed for at administrere hvilke brugere der har adgang til sikkerhedsgrupper og politikker i MS-AD.



Når en bruger får tildelt en Jobfunktionsrolle eller en Forretningsrolle sendes information om medlemskab tilbage til kommunens MS-AD.

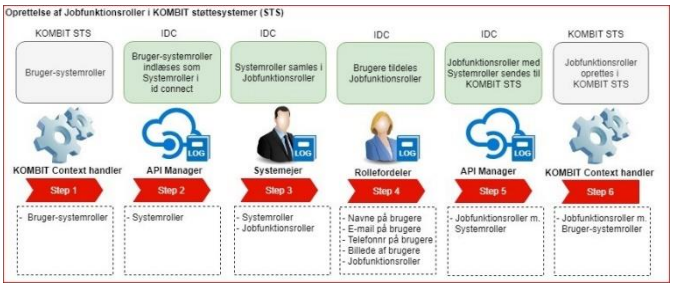
Det lokale MS-AD vil altid være opdateret, og adgang til interne systemer vil altid være tilgængelige, uanset om kommunikation til servicen hos ID Connect skulle være afbrudt.

ID Connect logger alle bruger- og rolle ændringer, og flytter samtidig både opgaven og ansvaret fra IT-afdelingen ud i forretningen. Rolletildelere og ledere får et løbende overblik, som ellers ofte skal bestilles via rapporter.

Identity Provider
Integration ind mod KOMBIT

ID Connect sættes op til at være Identity Provider (IdP) for KOMBIT og andre eksterne services.

Med ID Connect som IdP, ligger brugere og deres login oplysninger forsat i AD og når brugeren logger ind på et system, valideres brugeren op mod MS-AD uden at password gemmes hos ID Connect.



Når ID Connect fungerer som IdP for eksempelvis KOMBIT støttesystemerne, logger brugeren ind i et KOMBIT fagsystem og sendes via KOMBIT Context handleren, videre til ID Connect, som validerer brugeren op mod kommunens MS-AD.

Når brugeren er godkendt, sendes den via KOMBIT Context handleren tilbage til fagsystemet, med information om hvilke jobfunktionsroller og derved også systemroller, brugeren er tilknyttet.

PRIVACY BY DESIGN

Integration til Kommunens Active Directory bygger på samme sikkerhedsteknologi som benyttes til at forbinde Microsoft Azure AD og kommunens eget lokale MS-AD.

- Kommunen kan prioritere på felt niveau om der skal laves read-only, eller om brugerne skal kunne opdatere feltet ved hjælp af ID Connect´s brugergrænseflade.
- ID Connect har ikke brug for at replikere brugernes login og password for at fungere på tværs af de tilknyttede services.
- Modtager kommunen anmodning om at anonymisere en brugers data, kan personhenførbare data anonymiseres på tværs af servicen, uden at miste statistik.

Kontakt Jørgen Østergaard på jos@idconnect.dk eller på mobil 5363 6732 for mere information.

INFORMATIONSSIKKERHED

Med Persondataforordningen i 2018, kom der et øget fokus på det ansvar der følger med behandling af personhenførbare informationer.

Vores løsning forbedrer især overblikket for de aktører i kommunerne, der kan have svært ved at skabe et overblik over risici og status.

- Data- og systemejer
- Informationssikkerhedskoordinator
- Databeskyttelsesrådgiver (DPO)

Med brugen af KOMBITs rollemodel på tværs af andre services, får man den samme indsigt i hvilke brugere der har adgang til hvilke systemer.

En brugervenlig portal til rolletildelere og mellem-ledere, reducerer de aktuelt udstedte rettigheder, hvormed også risikoen reduceres i kommunen.

idconnect