

Hjem / Infrastrukturens løsninger / Adgangsstyring

Adgangsstyring for brugere

Adgangsstyring for brugere sikrer, at brugere kun tilgår de informationer, som de har fået tildelt rettigheder til af deres myndighed.

På denne side kan du læse om:

- [Hvad er Adgangsstyring for brugere](#)
- [Context Handler](#)
- [Ny version af Context Handler \(Context Handler 2\)](#)
- [Vejledninger til opsætning af adgangsstyring, jobfunktionsroller mm.](#)
- [Integrationer til Context Handler](#)
- [Certifikater](#)
- [Link til metadata for Context Handler 1 og Context Handler 2](#)
- [Vilkår for Adgangsstyring for brugere](#)
- [Testværktøjer](#)

Hvad er Adgangsstyring for brugere

Fælleskommunal Adgangsstyring for brugere foregår ud fra *autentifikation* og *autorisation*, som er styret i myndighedens brugerstyring.

- **Autentifikation** bestemmer brugerens identitet og hvilket tilhørsforhold, denne har til en myndighed.
- **Autorisation** er brugerens rettigheder - hvad må den pågældende bruger. Denne tildeling/afgrænsning af rettigheder styres med jobfunktionsroller og dataafgrænsninger.

En brugers rettigheder udtrykkes ved kombinationer af roller og afgrænsninger. Fx kan man udtrykke en rettighed som ”*du må læse dokumenter, men kun de dokumenter, der omhandler dagpenge*”:

Menu



eller ”som medarbejder må du se lønoplysninger, men kun i din egen afdeling”:

- Rolle: Se lønoplysninger
- Dataafgrænsning: Organisation UUID på brugerens organisation

Det vil sige, at en rettighed altid består af en rolle (hvad du må), og den kan eventuelt kombineres med en eller flere afgrænsninger (hvilke data du må udføre de tilladte handlinger på).

Adgangsstyring for brugere i den fælleskommunale infrastruktur er integreret med alle myndigheders Identity Providere, hvilket gør, at kommunens brugere automatisk kan logges på.

Context Handler

Context Handler er en SAML IdP-proxy, der udsteder adgang for brugere på vegne af de kommunale Identity Providere til de brugervendte systemer, der er registreret i den fælleskommunale infrastruktur. Brugervendte systemer er typisk fagsystemer, der har en brugergrænseflade (SAPA, BBR eller lignende).

Sikkerhedsmodellen understøttes af Context Handleren og Fælleskommunalt Administrationsmodul. Både det brugervendte system og kommunens lokale Identity Provider (IdP) integrerer til Context Handler, og begge systemer er registreret i Fælleskommunalt Administrationsmodul, hvor rettighederne modelleres i form af jobfunktionsroller. Det betyder, at det brugervendte system ikke kommunikerer direkte med kommunens lokale IdP, men at Context Handleren agerer proxy for kommunen og oversætter rettighederne mellem de to systemer.

Ny version af Context Handler – klar til NSIS og NemLog-in3

Nedenfor er samlet mere information om Context Handler 2 (tidligere kaldet NSIS-Context Handler), samt tidsplan for test og ibrugtagning.

Information om Context Handler 2

Ny funktionalitet i Context Handler 2

Menu



Hvad skal kommuner gøre for at skifte til Context Handler 2?

NemLog-in - OIOSAML 2 og OIOSAML 3

Udfasning af Context Handler 1

Kontrol af NSIS-revidering af IdP'er

Læs mere om NSIS

Vejledninger

Nedenstående vejledninger gennemgår, hvad der skal udføres for at kunne anvende Context Handleren:

- Sådan implementerer du single-sign-on: [Vejledning til Adgangsstyring for brugere](#)
- Kom godt i gang: [Tilslut brugervendt system](#)
- Lav jobfunktionsroller: [Vejledning til udarbejdelse af jobfunktionsroller for kommuner](#)
- Opsæt en Identity Provider: [Vejledning til opsætning af Identity Provider](#)
- Link til Fælleskommunal Administration for myndigheder: [Brugervejledning til Administrationsmodulerne for myndigheder](#)
- Eksempel: [metadata for brugervendt system](#)
- Eksempel: [metadata for Identity provider](#)

Skift af IdP SAML-metadata

Hvis du som myndighed skal skifte SAML-metadata på din tilsluttede IdP, fx hvis du skal opdatere certifikat, skal du gøre følgende:

- Planlæg skiftet, så det påvirker din organisations brugere mindst muligt - det er ikke muligt at undgå nedetid
- Dan nye SAML-metadata i jeres IdP – bemærk, at SAML-metadatafilen kun må indeholde ét certifikat

Menu



Upload nye IdP SAML-metadata på jeres registrerede IdP i Fælleskommunale Administrationsmodul (bemærk, at AD FS-metadata kan indlæses direkte i Administrationsmodulet uden ændringer, så længe det indeholder ét certifikat)

Herefter vil der gå et kort stykke tid, mens Administrationsmodulet lægger data over i Context Handler, derefter kan I igen bruge jeres IdP til at logge på.

Hvis I har behov for hjælp undervejs i processen, kan du kontakte [Serviceplatformens Helpdesk](#).

08:09

'Kom godt i gang'-vejledninger

Skal du integrere med den fælleskommunale infrastruktur for første gang? I vores nye serie 'Kom godt i gang', har vi udarbejdet en række trin-for-trin vejledninger, som du kan bruge, når du skal i gang med at anvende infrastrukturen.

[Find vejledningerne her](#) →

Menu



- [SF1515 - SAMLSingleLogout](#)

Certifikater

Du finder certifikaterne til den fælleskommunale infrastruktur på siden for [certifikater](#).

Hvis du ikke før har prøvet at anvende certifikater i infrastrukturen, så kan du finde hjælp i vores vejledning '[Kom godt i gang - certifikater](#)'.

Link til metadata

Bemærk, at der findes forskellig metadata til henholdsvis den gamle version (Context Handler 1) og den nye Context Handler 2.

Du finder metadata til hver version nedenfor.

Metadata til Context Handler 1 (gammel version)

Metadata Ekstern Test Context Handler 1:

- For brugervendt system: <https://adgangsstyring.ekstern-test-stoettesystemerne.dk/runtime/saml2/metadata.idp>
- For IdP (kommunal eller leverandørmyndighed): <https://adgangsstyring.ekstern-test-stoettesystemerne.dk/runtime/saml2auth/metadata.idp>

Metadata Produktion Context Handler 1:

- For brugervendt system: <https://adgangsstyring.stoettesystemerne.dk/runtime/saml2/metadata.idp>
- For kommunal IdP: <https://adgangsstyring.stoettesystemerne.dk/runtime/saml2auth/metadata.idp>

Metadata til Context Handler 2 (ny version)

Metadata Ekstern Test Context Handler 2:

Menu



For IdP (kommunal eller

leverandørmyndighed): <https://n2adgangsstyring.eksterntest-stoettesystemerne.dk/runtime/saml2auth/metadata.idp>

Metadata Produktion Context Handler 2:

- For brugervendt system: <https://n2adgangsstyring.stoettesystemerne.dk/runtime/saml2/metadata>.
- For kommunal IdP: <https://n2adgangsstyring.stoettesystemerne.dk/runtime/saml2auth/metadata>

Vilkår for Adgangsstyring for brugere

Det er nødvendigt, at vilkår for anvendelse af sikkerhedsmodellen i den fælleskommunale rammearkitektur anvendes.

Læs vilkår for [anvendelse af sikkerhedsmodellen](#) og [beskrivelsen af sikkerhedsmodellen](#).

Læs [servicebeskrivelse og vilkår for Context Handler 2](#).

Testværktøjer

KOMBIT stiller testværktøjer til rådighed for myndigheder til test af IdP'er. Testværktøjerne giver mulighed for at inspicere login-flowet i en browser i forbindelse med test af Adgangsstyring i det eksterne testmiljø. Bemærk, at der er forskellige testværktøjer til henholdsvis Context Handler 1 og til Context Handler 2.

Testværktøj til Context Handler 1

- Til test med NIST-sikringsniveauer: <https://demo-brugervendtsystem.kombit.dk/test/>

Bemærk, at der ikke er fastsat en SLA for testværktøjets tilgængelighed og at evt. fejl skal indrapporteres til FKI@kombit.dk.

Testværktøjer til Context Handler 2

Eksternt testmiljø

- Til test i Eksternt testmiljø med NIST-sikringsniveauer: <https://spwithoutnsis.eksterntest-stoettesystemerne.dk/>

Menu



Produktionsmiljø

- Til test i Produktionsmiljø med NIST-sikringsniveauer: <https://spwithoutnsis.stoettesystemerne.dk/>
- Til test i Produktionsmiljø med NSIS-sikringsniveauer: <https://spwithnsis.stoettesystemerne.dk/>

DIGITALISERINGS KATALOGET

Fælleskommunal infrastruktur

Kontakt og support

Om den fælleskommunale infrastruktur

Fælleskommunalt Administrationsmodul

Om Digitaliseringskataloget

Privatlivspolitik

Cookiepolitik

Tilgængelighedserklæring

Vilkår og aftaler

Generelle vilkår

Tekniske betingelser

SKI 02.19 og infrastrukturen

Kontakt os

FKI@kombit.dk

Menu



KOMBIT A/S

Halfdansgade 8

2300 København S

CVR-nr.: 19435075

EAN-nr.: 5790001969370