Digitaliseringsstyrelsen

DATAAFGRÆNSNINGER

Sådan implementerer I som it-systemudbyder/it-leverandør dataafgrænsninger

Version: 1.0

Forfatter: Digitaliseringsstyrelsen, NemLog-in

NemLog-in

Indholdsfortegnelse

Dokumenthistorik

Version	Dato	Forfatter	Bemærkninger
1.0	april 2026	Digitaliseringsstyrelsen	Den første version.

1. Introduktion

1.1. Formål

Formålet med dette materiale er at vejlede it-systemudbyder i anvendelsen af dataafgrænsninger, som administreres i NemLog-in Administration:

https://administration.nemlog-in.dk/.

Materialet beskriver de tekniske aspekter ved opsætning, konfiguration og udstilling af dataafgrænsninger samt den tilhørende dokumentation i forbindelse med integration og implementering.

Materialet giver indsigt i de muligheder og nødvendige overvejelser, der er i forbindelse med ibrugtagning af dataafgrænsninger.

I forbindelse med implementering af dataafgrænsninger, har vi brug for en række informationer. Derfor skal I som it-systemudbydere orientere jer i nedenstående sider.

1.2. Målgruppe

Materialet er målrettet it-systemudbydere og it-leverandører, der arbejder med integration af it-systemer til NemLog-in, herunder tilslutning, konfiguration og administration. Materialet er særlig relevant for udbydere af it-systemer, som allerede opererer med privilegier, som tilknyttes og udstilles som rettigheder/fuldmagter i MitID Erhverv eller fuldmagter i Digital Fuldmagt og som ønsker anvendelse af dataafgrænsninger.

Dataafgrænsninger i NemLog-in kan anvendes til at indsnævre betydningen af en rettighed eller fuldmagt ved at kunne afgrænse til eksplicitte forretningsobjekter, der defineres af it-systemudbyderens kontekst. Det kan fx være en sag identificeret ved et sagsnummer.

1.3. Afgrænsning

Materialet omhandler primært den tekniske implementering og håndtering af dataafgrænsninger. Materialet har *ikke* til formål at vejlede i eller understøtte en it-systemudbyderens forretningsmæssige vurdering af, hvorvidt implementering af dataafgrænsninger er relevant eller hensigtsmæssig for it-systemudbyderens it-system. En eventuel beslutning herom træffes alene af den enkelte it-systemudbyder med udgangspunkt i egne forretningsmæssige behov, forretningsregler samt organisatoriske rammer.

Materialet giver indsigt i de tekniske muligheder og overvejelser, der bør indgå i forbindelse med ibrugtagning af dataafgrænsninger. Hvor det er relevant, henvises der til yderligere materiale og dokumentation via links.

1.4. Forudsætning

Det forudsættes, at læseren har grundlæggende kendskab til NemLog-in Administration, herunder håndtering af privilegier, rettigheder og fuldmagter samt erfaring med systemintegration og SAML-autentifikation via NemLog-in, ellers henvises der til at læse mere i brugermanualen til NemLog-in Administration:

https://cms.nemlog-in.dk/media/slibbjiv/brugermanual-til-nemlog-in-administration.pdf

For at kunne anvende dataafgrænsninger kræver det, I skal være tilsluttet NemLog-in som it-systemudbyder og have oprettet et it-system i NemLog-in Administration. De fleste er allerede tilsluttet og har oprettet et it-system.

Er I endnu ikke er tilsluttet NemLog-in, kan I læse mere om tilslutning her:

https://www.nemlog-in.dk/tilslutning/

Hvis I er tilsluttet, kan I logge ind i NemLog-in Administration her:

https://administration.nemlog-in.dk/

2. Begrebsafklaring

Dette afsnit definerer centrale begreber, som anvendes i forbindelse med privilegier og dataafgrænsninger i NemLog-in. Formålet er at sikre en fælles forståelse af terminologien på tværs af myndigheder og tekniske implementeringer. Dette med særlig fokus på NemLog-ins rettighedsmodel samt de tekniske løsninger, hvis brugergrænseflade vil blive påvirket ved implementering af dataafgrænsninger.

2.1. NemLog-ins rettighedsmodel og privilegier

NemLog-in anvender en rettighedsmodel, som tillader myndigheder at administrere privilegier koblet til deres it-systemer. Et privilegium er en logisk entitet, som udgør en specifik adgang, som tildeles via en rettighed eller fuldmagt i MitID Erhverv eller en fuldmagt via Digital Fuldmagt. Privilegier kan således give adgang til både selvbetjeninger og andre former for interaktion med myndigheden fx telefonisk eller skriftligt.

Privilegier kan indgå i og definere en specifik adgang på følgende måder:

- i en rettighed som tildeles erhvervsbrugere via MitID Erhverv
- som rettigheder i en erhvervsfuldmagt via MitID Erhverv
- som fuldmagter fra borgere via Digital Fuldmagt
- som fuldmagter fra MitID Privat til Erhverv brugere via Digital Fuldmagt.

Myndigheden har ansvar for at definere, hvad et privilegium giver adgang til, og må beslutte om fx:

- privilegiet skal give adgang til hele eller dele af en digital selvbetjeningsløsning eller sagsområde
- der skal oprettes flere privilegier for at dække delmængder eller specifikke sagsområder af den digitale selvbetjeningsløsning.

Privilegier konfigureres og administreres af den ansvarlige for integrationen af it-systemet i NemLog-in Administration. Brugerens tildelte privilegier indgår som en del af brugerens autentifikationssvar i SAML-billetten eller hentes af it-systemudbyderen ved hjælp af API.

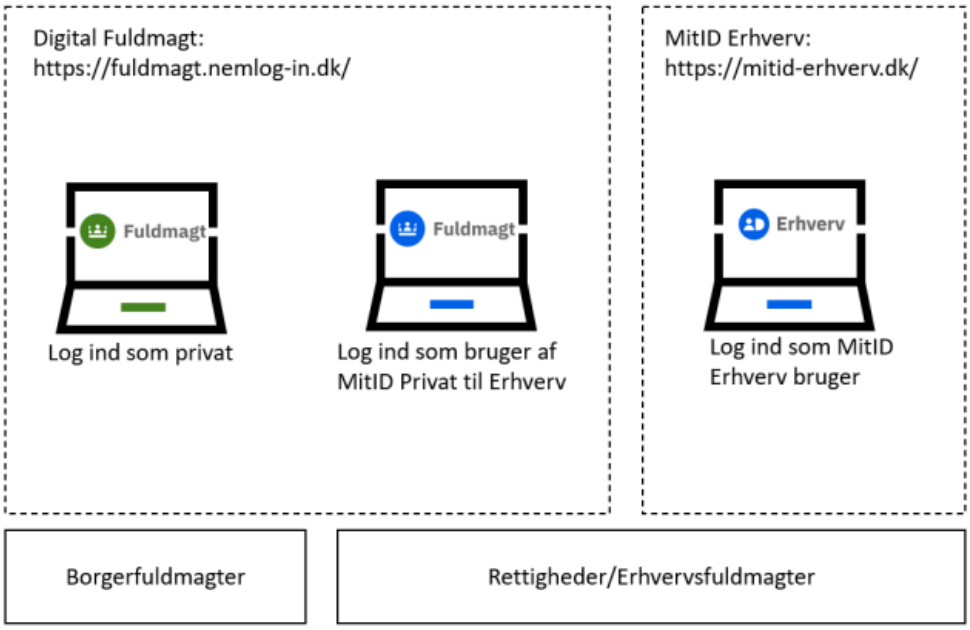
Anvender I allerede NemLog-ins rettighedsmodel og privilegier, og ønsker I udvidelse med dataafgrænsninger, kan I læse videre her.

Hvis I ikke anvender NemLog-ins rettighedsmodel og privilegier, men ønsker at gøre brug af det, kan I læse mere her:

https://www.nemlog-in.dk/

2.2. Opdelingen mellem de tre løsninger i NemLog-in

Digitaliseringsstyrelsen driver tre tekniske løsninger i NemLog-in. Nedenstående figur har til formål at illustrere opdelingen:



Løsningerne er rettet mod borgere, brugere af MitID Privat til Erhverv og slutteligt en løsning rettet mod brugere af MitID Erhverv.

2.3. Rettigheder MitID Erhverv

En rettighed er en adgang eller ret til at udføre bestemte opgaver i en offentlig selvbetjeningsløsning. Rettigheder udstilles og tildeles brugere i MitID Erhverv. Det kan fx være en rettighed til NemRefusion for at anmode om refusion på vegne af organisationen. Rettigheden tildeles f.eks. en HR-medarbejder, som skal sikre at indberetning af NemRefusion for organisationen varetages.

Myndigheder, som ikke tilbyder rettigheder for erhvervsbrugere, men ønsker at give de organisationer, der bruger jeres it-system, fx selvbetjening, mulighed for i MitID Erhverv at styre, hvem der har adgang til hvad i jeres løsning, kan læse mere her:

https://www.nemlog-in.dk/rettigheder

Yderligere oplysninger om rettigheder og MitID Erhverv findes her:

https://mitid-erhverv.dk/rettigheder

Spørgsmål til oprettelse af rettigheder kan stiles til MitID Erhverv i Digitaliseringsstyrelsen på mailadressen: **mitiderhverv@digst.dk**

2.4. Erhvervsfuldmagter MitID Erhverv

Organisationer som er tilsluttet MitID Erhverv kan anmode om eller afgive erhvervsfuldmagter i MitID Erhverv. Erhvervsfuldmagter indeholder rettigheder, der afgives fra én organisation til en anden. De rettigheder, der kan afgives som erhvervsfuldmagter i MitID Erhverv, kan også anvendes af brugere af

MitID Privat til Erhverv i Digital Fuldmagt. Læs mere om Fuldmagter for MitID Privat til Erhverv i afsnittet *'Digital Fuldmagt for MitID Privat til Erhverv'* nedenfor.

Myndigheder, som ikke tilbyder rettigheder som, indgår i erhvervsfuldmagter for erhvervsbrugere, men ønsker at give de organisationer, der bruger jeres it-system, fx selvbetjening, mulighed for i MitID Erhverv at styre, hvem der har adgang til hvad i jeres løsning, kan læse mere her:

https://www.nemlog-in.dk/rettigheder

Spørgsmål herom kan stiles til MitID Erhverv i Digitaliseringsstyrelsen på mailadressen:
mitiderhverv@digst.dk

2.5. Digital Fuldmagt MitID Privat til Erhverv

Personer, der driver en enkeltmandsvirksomhed eller en personligt ejet mindre virksomhed, kan anvende deres private MitID til erhvervsmæssige formål (MitID Privat til Erhverv). Dette gælder ligeledes for ejere af et anpartsselskab (ApS) eller et aktieselskab (A/S), såfremt ejeren kan tegne virksomheden alene.

I sådanne tilfælde har virksomheden som udgangspunkt ikke behov for tilslutning til MitID Erhverv, og kan således anvende den erhvervsrettet brugergrænseflade i Digital Fuldmagt i forbindelse med anmodning eller afgivelse af erhvervsfuldmagter.

Ved log-in anvendes privat MitID til at logge ind med rollen 'ledelsesrepræsentant' og erhvervsfuldmagter kan oprettes i den er erhvervsrettede Digital Fuldmagt brugergrænseflade. Det er myndigheden, som udbyder af et it-system, der beslutter, hvorvidt en fuldmagt skal være tilgængelig eller ej. Hvis man er ansat i en organisation som benytter MitID Erhverv, skal erhvervsfuldmagter oprettes i MitID Erhverv.

Myndigheder, som ikke tilbyder digital fuldmagt for MitID Privat til Erhverv-brugere, men ønsker at give de organisationer, der bruger jeres it-system, fx selvbetjening, mulighed for dette, kan læse mere her:

https://www.nemlog-in.dk/rettigheder

Spørgsmål til oprettelse af rettigheder kan stiles til MitID Erhverv i Digitaliseringsstyrelsen på mailadressen:

mitiderhverv@digst.dk

2.6. Digital Fuldmagt Borger

Digital Fuldmagt for borger gør det muligt for offentlige myndigheder at tilbyde borgere fuldmagt til blandt andet myndighedens digitale selvbetjeninger. Det betyder, at en borger med en digital fuldmagt kan få lov til at handle på en andens borgers vegne – og at borgere med behov for digital støtte kan få hjælp på lovlig vis. Dette foregår i den borgerettede brugergrænseflade, hvor borgere logger på med deres private MitID.

Myndigheder som ikke tilbyder fuldmagtspakker i digital fuldmagt for borger, men ønsker at give borgere mulighed for at oprette fuldmagter til jeres løsning, kan læse mere her:

https://www.nemlog-in.dk/digital-fuldmagt/

Spørgsmål til oprettelse af fuldmagtspakker i Digital Fuldmagt, kan stiles til Digital Fuldmagt i Digitaliseringsstyrelsen på mailadressen:

digitalfuldmagt@digst.dk

3. Krav for anvendelse af dynamisk dataafgrænsning

Hvis I som myndighed ønsker at anvende dynamisk dataafgrænsning, skal I være opmærksomme på følgende krav for anvendelse af dynamisk dataafgrænsning i NemLog-in.

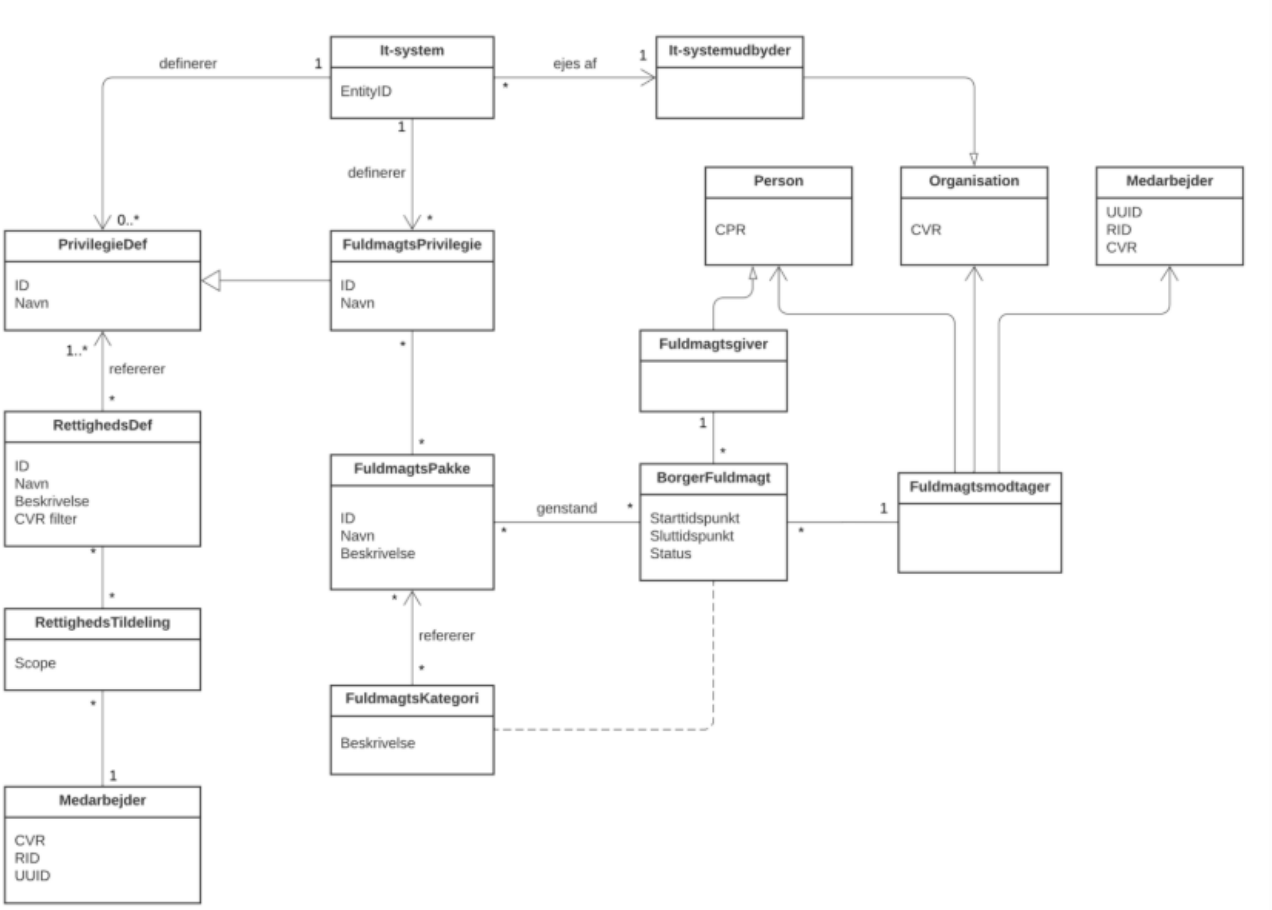
Krav	Beskrivelse
Dataafgrænsningnsmæssige parametre må *ikke* anvendes til at udstilles følsomme personoplysninger	Myndigheder som ønsker at tage dataafgrænsning i brug skal være opmærksomme på, at det *ikke* er tilladt at anvende dynamisk dataafgrænsning til at udstille personoplysninger, der er omfattet af forbuddet i databeskyttelsesforordningens artikel 9, stk. 1. Dette betyder blandt andet, at fx journaltitler, der angår specifikke sundhedsforhold, *ikke* må udstilles via dynamisk dataafgrænsning. Dette skyldes, at Digitaliseringsstyrelsen ikke har hjemmel til behandling af følsomme personoplysninger i Digital Fuldmagt eller MitID Erhverv.
Særligt for borgere: Det skal være *frivilligt* at udfylde dataafgrænsning på borgerfuldmagter.	Myndigheder som ønsker at tage dataafgrænsning i brug skal være opmærksomme på, at det *ikke* er tilladt at anvende dynamisk dataafgrænsning til at udstille personoplysninger, der er omfattet af forbuddet i databeskyttelsesforordningens artikel 9, stk. 1. Dette betyder blandt andet, at fx journaltitler, der angår specifikke sundhedsforhold, *ikke* må udstilles via dynamisk dataafgrænsning. Dette skyldes, at Digitaliseringsstyrelsen ikke har hjemmel til behandling af følsomme personoplysninger i Digital Fuldmagt eller MitID Erhverv.

4. Modellering af dataafgrænsninger

4.1. Grundlag for udvidelse af den eksisterende rettighedsmodel i NemLog-in

Den tidligere rettighedsmodel i NemLog-in var forholdsvis enkel. Privilegier, rettigheder og fuldmagtspakker var opbygget som éndimensionelle og statiske, og medførte en række begrænsninger i forhold til, hvor detaljeret og præcist disse kunne defineres. Rettigheder og fuldmagter fungerede som et på forhånd defineret sæt af "mærkater", der kunne tilknyttes en bruger eller borger, men de kunne ikke anvendes til at pege på dynamiske eller kontekstafhængige forretningsobjekter såsom sager, dokumenter eller foldere, uden at der skulle oprettes separate rettigheder eller fuldmagter for hver enkelt kombination af adgangsbehov.

Nedenfor er den tidligere rettighedsmodel i NemLog-in illustreret i UML. Modellen dækker både almindelige rettigheder samt fuldmagtspakker. Illustrationen er forenklet, hvorfor enkelte aspekter, som vurderes ikke relevant for fremstillingen, er udeladt (herunder erhvervsfuldmagter, delte privilegier og grupper).



Udvidelsen af rettighedsmodellen i NemLog-in introducerer *dataafgrænsninger*, der muliggør øget fleksibel og finkornet adgangsstyring. En dataafgrænsning giver myndigheder og it-systemudbydere mulighed for at tilføje afgrænsninger til et privilegium, som enten begrænser eller præciserer, hvilke data eller objekter der kan tilgås via en rettighed eller fuldmagt. Samtidig reduceres myndigheders og it-systemudbydere behov for lokale tilpasninger og proprietære adgangsmodeller, der tilsammen medvirker til en mere forenklet løsning for slutbrugeren.

4.2. Udvidelse af NemLog-ins rettighedsmodel

Den tidligere rettighedsmodel i NemLog-in omfatter nu en ny entitet: *dataafgrænsningstyper*. Dataafgrænsningstyper har til formål at modellere afgrænsninger for en myndighed eller it-systemudbydere, således håndtering af specifikationer af afgrænsninger for privilegier udvides. Håndteringen af dataafgrænsninger er bagudkompatibel, således udvidelsen ikke påvirker eksisterende it-systemer tilsluttet NemLog-in.

I modellen hænger dataafgrænsningstyperne på privilegierne, som er defineret i det pågældende it-system. Dette grundet kun it-systemerne ved, hvilke dataafgrænsninger, de forstår i deres håndhævelse af adgange. På den måde vil it-systemer gennem NemLog-in kun modtage de privilegier og dataafgrænsninger, som myndigheden eller it-systemudbyderen selv har erklæret, at de forstår. Der pålægges derfor et større ansvar hos den enkelte myndighed og it-systemudbyderen, som ønsker dataafgrænsninger.

Modellen fungerer således, at der på privilegiet angives, at der er tilknyttede dataafgrænsninger, som indsnævrer virkefeltet for privilegiet. Dataafgrænsninger kan komme i spil på to måder:

- Ved *definitionen* når et privilegie eller rettighed oprettes skal man kunne tilknyttet en eller flere dataafgrænsningstyper
- Ved *tildelingen* af en rettighed eller fuldmagt skal it-systemet bede om værdien for hver tilknyttet *instans* af dataafgrænsning.

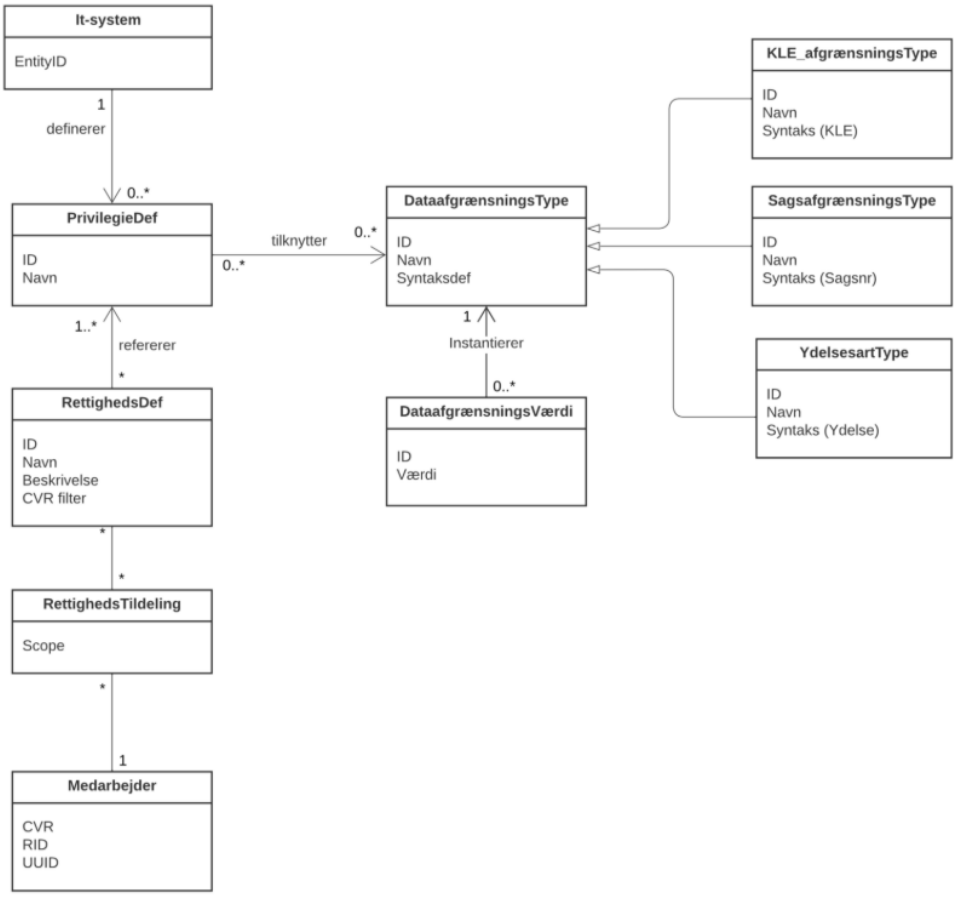
Dataafgrænsninger kan anvendes på almindelige/medarbejder- og borgerprivilegier. Læs mere om, hvilke juridiske opmærksomhedspunkter I bør være opmærksomme på, inden I påbegynder anvendelse af dataafgrænsninger, under punkt 3. Krav for anvendelse af dynamisk dataafgrænsning.

Nedenfor er et simplificeret eksempel af almindelige/medarbejder privilegier illustreret i UML:

Forklaring af eksemplet

et it-system definerer privilegiet ”Se sag”, som giver læseadgang til sager i et system eller domæne (fx byggesager). Ved oprettelse af privilegiet kan it-systemudbyderen oprette en dataafgrænsningstype kaldet ”sagsafgrænsning” indeholdende feltet ”sagsnummer”. Ved at tilknytte dataafgrænsningen til privilegiet, skal der ved tildeling af enten rettigheden til en bruger eller i en erhvervsfuldmagt i MitID Erhverv, angives værdien af en eller flere sagsnumre, som indsnævrer læseadgangen (rettigheden) til det eller de angivne sagsnumre. Således opnås en mere detaljeret styring af adgang med flere dimensioner, hvor rettigheden siger noget om, hvad brugeren må gøre, og dataafgrænsningerne yderligere specificerer *på hvad* rettigheden må anvendes til.

Nedenfor vises den generaliserede model, som kan håndtere vilkårlige dataafgrænsningstyper (modellen viser tre konkrete dataafgrænsningstyper: KLE, sagsnumre og ydelsesarter):



Vær opmærksom på at dette eksempel illustrerer et casescenarie rettet mod erhverv. Der findes tilsvarende eksempel for borger længere nede i afsnittet.

Bemærk, såfremt et privilegie eller en rettighed tilknyttes flere dataafgrænsninger, gælder fællesmængden af dataafgrænsninger. Det betyder, at det kun er de dataobjekter, der opfylder alle kriterier i alle dataafgrænsninger, som privilegiet / rettigheden kan anvendes på.

4.3. Dataafgrænsningsmetoder: validering

Der tilbydes to former for valideringsmetoder, herunder statisk- og callback validering. Således kan dataafgrænsninger fortolkes som key-value par af *type* og *værdi*. Værdien af en dataafgrænsning udfyldes ved tildeling af en rettighed eller fuldmagt og skal overholde det tilhørende 'adresserum'.

4.4. Statisk validering

Der kan angives et tekstfelt med et tilhørende regulært udtryk, som definerer de syntaktiske lovlige værdier for dataafgrænsningen. I nogle scenarier er dette fordelagtig. Dette gælder eksempelvis i situationer, hvor dataafgrænsningen har faste værdier eller en fast struktur.

Eksempler på dette kendes fra den fælleskommunale adgangsstyring, hvor der anvendes dataafgrænsninger på følsomhed, der angives i intervallet 1-4 eller dataafgrænsninger på KLE-værdier, som har en fast struktur som fx "27.1.20". Ved anvendelse af regulære udtryk sikrer MitID Erhverv og Digital Fuldmagt, at brugeren indtaster en syntaktisk lovlig værdi for dataafgrænsningen ved tildeling af en rettighed eller fuldmagt.

Statisk validering via regulært udtryk er lettest at implementere og introducerer færrest mulige afhængigheder mellem NemLog-in og it-systemudbyderen. Til gengæld giver metoden ikke mulighed for at operere med dataafgrænsninger, hvor værdisættet er afhængigt af bruger eller kontekst. I disse tilfælde skal der i stedet anvendes callback validering som beskrevet nedenfor.

Det er vigtigt, at den ønskede værdi beskrives i "Kort beskrivelse af dataafgrænsningen", så slutbrugerne ved præcis, hvordan de skal udfylde dataafgrænsningen. Fx hvilket format en dato skal noteres i, eksempelvis dd-mm-åååå eller dd.mm.åå.

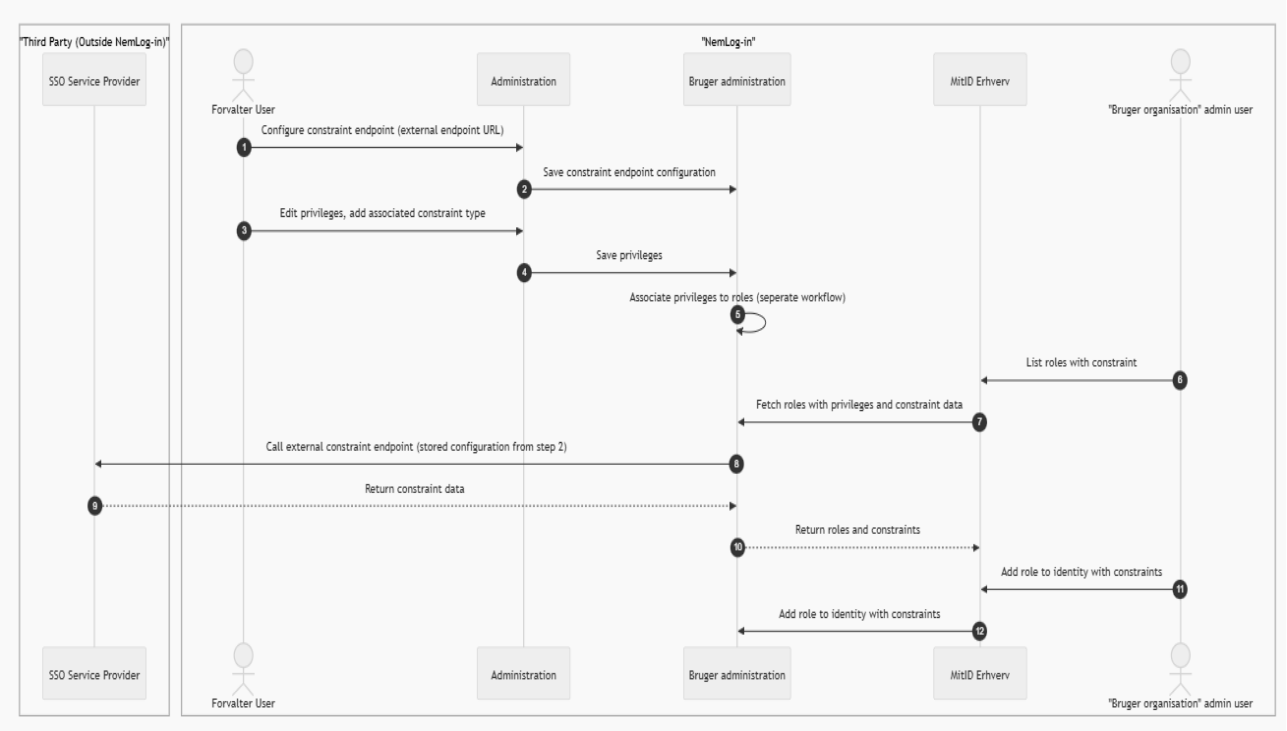
4.5. Callback-validering

Der kan angives en URL til myndighedens eller it-systemudbyderens callback-service, hvor NemLog-in i forbindelse med tildeling af en rettighed eller fuldmagt ved run-time, henter en liste over de aktuelle værdier for den specifikke dataafgrænsning og den aktuelle bruger.

Et eksempel kunne være et medarbejderprivilegie, der giver adgang til indberetning af moms for et specifikt SE-nummer, tilhørende en virksomhed. Her vil en callback-service, udstillet af det it-system, der anvender privilegiet, kunne anvendes til at validere, hvorvidt et givent SE-nummer tilhører virksomheden (defineret ved et CVR-nummer).

Et andet eksempel kunne være en borger, der tildeler en byggerådgiver adgang til at håndtere en byggesag på borgerens vegne i en kommunes sagsbehandlingssystem. Her kan en callback-service anvendes til at validere, at det kun er borgerens byggesager, der kan tildeles fuldmagt til at håndtere.

Nedenstående har til formål at illustrere forvaltning (opsætning) og flowet (anvendelse) for anvendelse af constraint/dataafgrænsning callback.



Læs den tekniske guide om, hvordan callback implementeres. Guiden er på engelsk og hedder: ”Retrieving constraint values through call-back service”.

https://cms.nemlog-in.dk/media/ojyc2prz/retrieving-constraint-values-through-call-back-service.pdf

5. Dataafgrænsninger i NemLog-in administration

Nedenfor beskrives en række brugerrejser, som bidrager til at give læseren en funktionel beskrivelse af, hvordan dataafgrænsninger fungerer i NemLog-in. For hver enkelt brugerrejse er det markeret, hvilken komponent i NemLog-in som påvirkes, og hvordan den specifikke brugergrænseflade påvirkes.

5.1. Ibrugtagning af dataafgrænsninger

For at myndigheder kan anvende dataafgrænsninger, kræver det at myndigheden er tilsluttet NemLog-in som it-systemudbyder og har oprettet et it-system i NemLog-in Administration. De fleste myndigheder er allerede tilsluttet og har oprettet et it-system.

Er I en myndighed, som endnu ikke er tilsluttet NemLog-in, kan I læse mere om tilslutning her:

https://www.nemlog-in.dk/tilslutning

Er I en myndighed, som allerede er tilsluttet, kan I logge ind i NemLog-in Administration her:

https://administration.nemlog-in.dk/

En dataafgrænsning skal oprettes på it-systemudbyderniveau, således afgrænsningen kan anvendes på flere it-systemer samtidig, alt efter behov. Derfor kan en afgrænsning tilknyttes it-systemer, som allerede har oprettet og anvender privilegier, samt systemer som endnu ikke gør brug af privilegier.

Vær opmærksom på, at hvis en dataafgrænsning tilknyttes et allerede eksisterende privilegie, som fx definerer en fuldmagtspakke i Digital Fuldmagt, hvortil der allerede er oprettet borgerfuldmagter, vil afgrænsningen kun gøre sig gældende for fremadrettede fuldmagter. Det betyder, at allerede eksisterende borgerfuldmagter fortsat er aktive, men uden en dataafgrænsning.

Myndigheder, der ønsker at tilknytte en dataafgrænsning til et allerede eksisterende privilegie, skal derfor væres særligt opmærksomme på, hvordan de allerede eksisterende fuldmagter, der er oprettet før dataafgrænsningen, er tilknyttet, bliver tolket og håndteret i egen adgangsstyring. Samme gør sig gældende ved erhvervsfuldmagter.

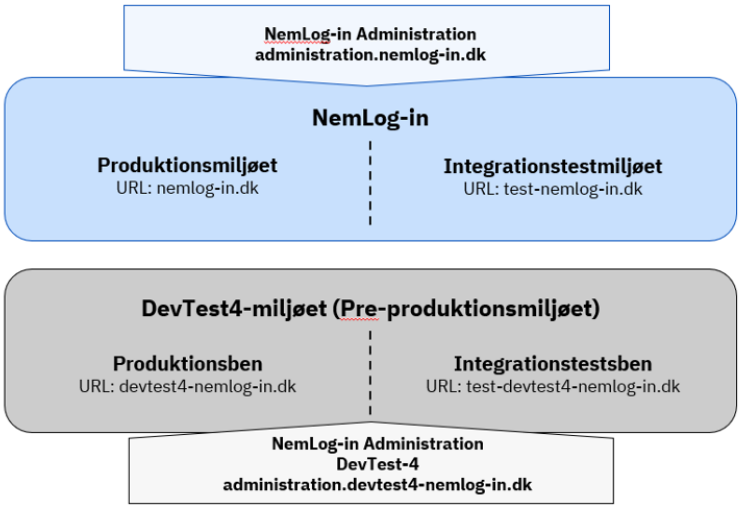
5.2. Oprettelse af dataafgrænsninger i NemLog-ins testmiljøer

Forud for at it-systemudbydere og it-leverandører, som arbejder med integration af it-systemer til NemLog-in kan implementere dataafgrænsninger, skal det sikres, at dataafgrænsningen er afprøvet i et testmiljø for at reducere risiko, sikre kvalitet og undgå fejl.

Ud over produktionsmiljøet findes der to testmiljøer:

- Integrationsmiljøet (afspejler produktion)
- Pre-produktionsmiljøet (devtest4 som inkluderer kommende funktionalitet)

Nedenstående figur illustrerer NemLog-ins 3 forskellige miljøer.



I kan læse mere om miljøerne her:

https://www.nemlog-in.dk/miljoer

Det er it-systemudbyderen, som beslutter, hvilket miljø de ønsker at teste op mod, men nedenstående anbefales:

- for Digital Fuldmagt at teste i integrationstestmiljøet
- for MitID Erhverv at teste i DevTest4.

Når man som it-systemudbyder vil teste dataafgrænsninger, skal man starte med at afgøre, om det er ønsket at teste mod en egenudviklede constraint service, eller om der vil blive anvendt NemLog-ins testudgave. Krav til egenudviklede constraint service er beskrevet i *Guide to implement constraint callback*, se [IMPL]. I samme guide er der beskrevet, hvor man kan finde NemLog-in testservicen.

Afsnittet *Oprettelse af dataafgrænsninger i NemLog-in produktion* har en tilsvarende fremgangsmetode som ved anvendelse af et testmiljø. Ved oprettelse af dataafgræsninger følges trin-for-trin-vejledningen nedenfor. Sørg dog for, at de korrekte test-URL'er, som illustreret i figuren, anvendes.

5.3. Oprettelse af dataafgrænsninger i NemLog-in i produktion

Dette er en trin-for-trin-vejledning til it-systemudbydere og it-leverandører, som arbejder med integration af it-systemer til NemLog-in, der ønsker opsætning af dataafgrænsninger. Håndtering af de tekniske data udføres af en teknisk administrator. Den tekniske administrator kan enten være medarbejder i

myndigheden, som udbyder it-systemet (it-systemudbyder) eller en medarbejder hos it- leverandøren, som har fået til opgave at stå for de tekniske konfigurationer.

For at kunne anvende dataafgrænsning i praksis skal organisationen foretage den nødvendige opsætning i NemLog-in administration. Opsætningen omfatter bl.a.:

- Oprettelse og vedligeholdelse af relevante rettigheder og roller
- Tildeling af dataafgrænsning til brugere eller systemer
- Eventuel håndtering af godkendelsesflows afhængigt af organisationens opsætning

For en trin-for-trin vejledning henvises til den gældende brugermanual for NemLog-in administration hvor opsætning, godkendelser og øvrige administrative processer er beskrevet i detaljer:

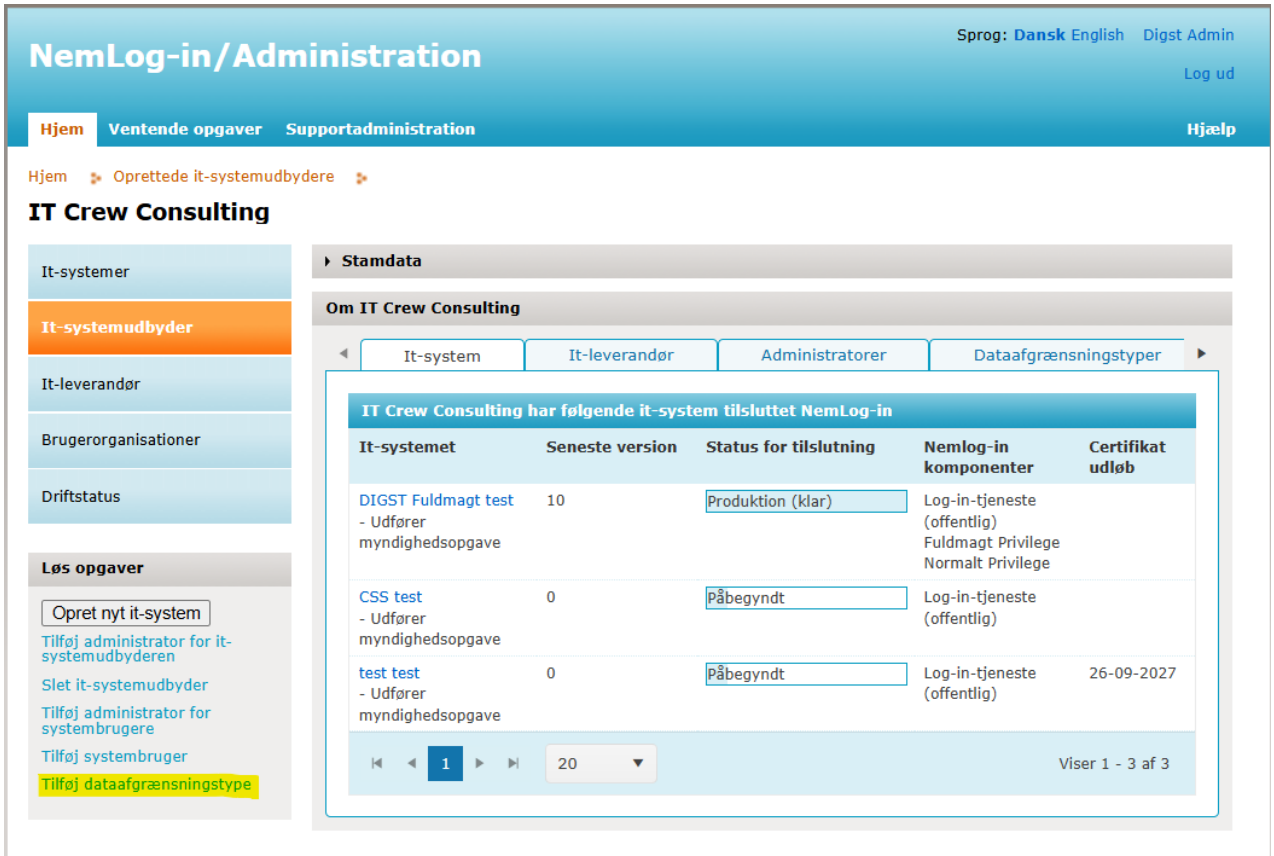
https://cms.nemlog-in.dk/media/slibbjiv/brugermanual-til-nemlog-in-administration.pdf

Ved oprettelse af dataafgrænsningstyper udføres nedenstående i NemLog-in Administration:

Opret dataafgrænsning

Ansvarlig: Administrator for it-systemudbyder

Administrator for it-systemudbyder skal under ventende opgaver, tilføje data afgrænsningstype:



Vær opmærksom på at den tekniske administrator ikke kan varetage denne del af opsætning af dataafgrænsninger, da oprettelsen skal varetages af Administrator for it-systemudbyder. Den tekniske administrator kan herefter stå for det resterende set-up af dataafgrænsninger på it-systemet.

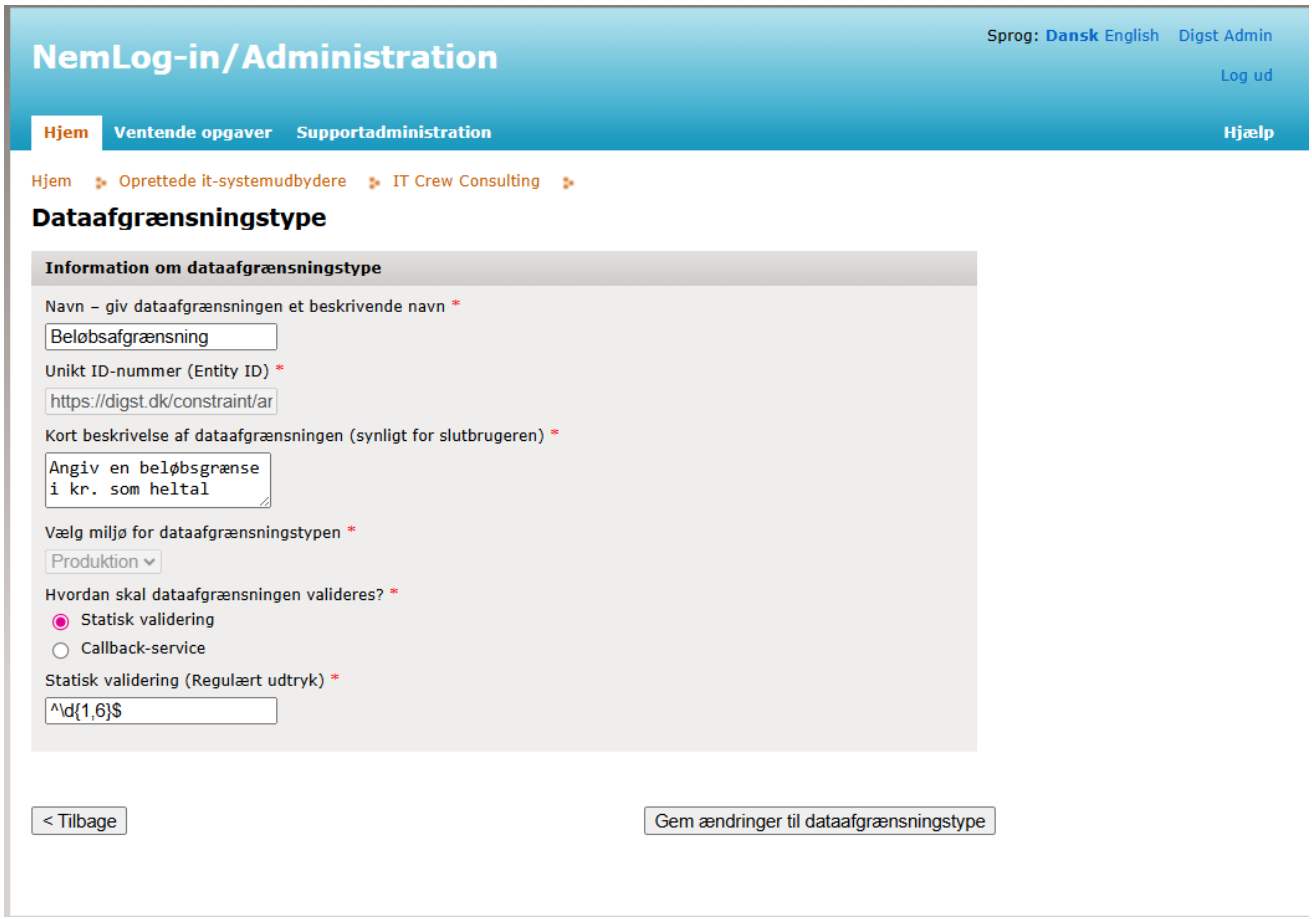
Opret dataafgrænsning med statisk validering

Ansvarlig: Administrator for it-systemudbyder

Som administrator for it-systemudbyderen skal du initiere oprettelsen af dataafgrænsningen. Sikre derfor:

1. Et beskrivende navn for dataafgrænsningen efterfuldt af et unikt ID-nummer (EntityID).
2. En kort beskrivelse af dataafgrænsningen. Vær opmærksom på at denne beskrivelse er synlig for slutbrugeren. Beskrivelsen skal indeholde det ønskede format for det regulære udtryk, fx, hvilket format en dato skal noteres i; dd-mm-åååå eller dd.mm.åå osv.
   Det er vigtigt, at den ønskede værdi beskrives i den korte beskrivelse af dataafgrænsningen, så slutbrugerne ved præcis, hvordan de skal udfylde dataafgrænsningen. Fx hvilket format en dato skal noteres i, eksempelvis dd-mm-åååå eller dd.mm.åå.
3. Valg af miljø samt valideringsmetode og indsæt slutvis et regulært udtryk for den statisk validering.
4. At ændringerne gemmes.

Se eksempel på en udfyldt dataafgrænsningstype med statisk validering nedenfor:



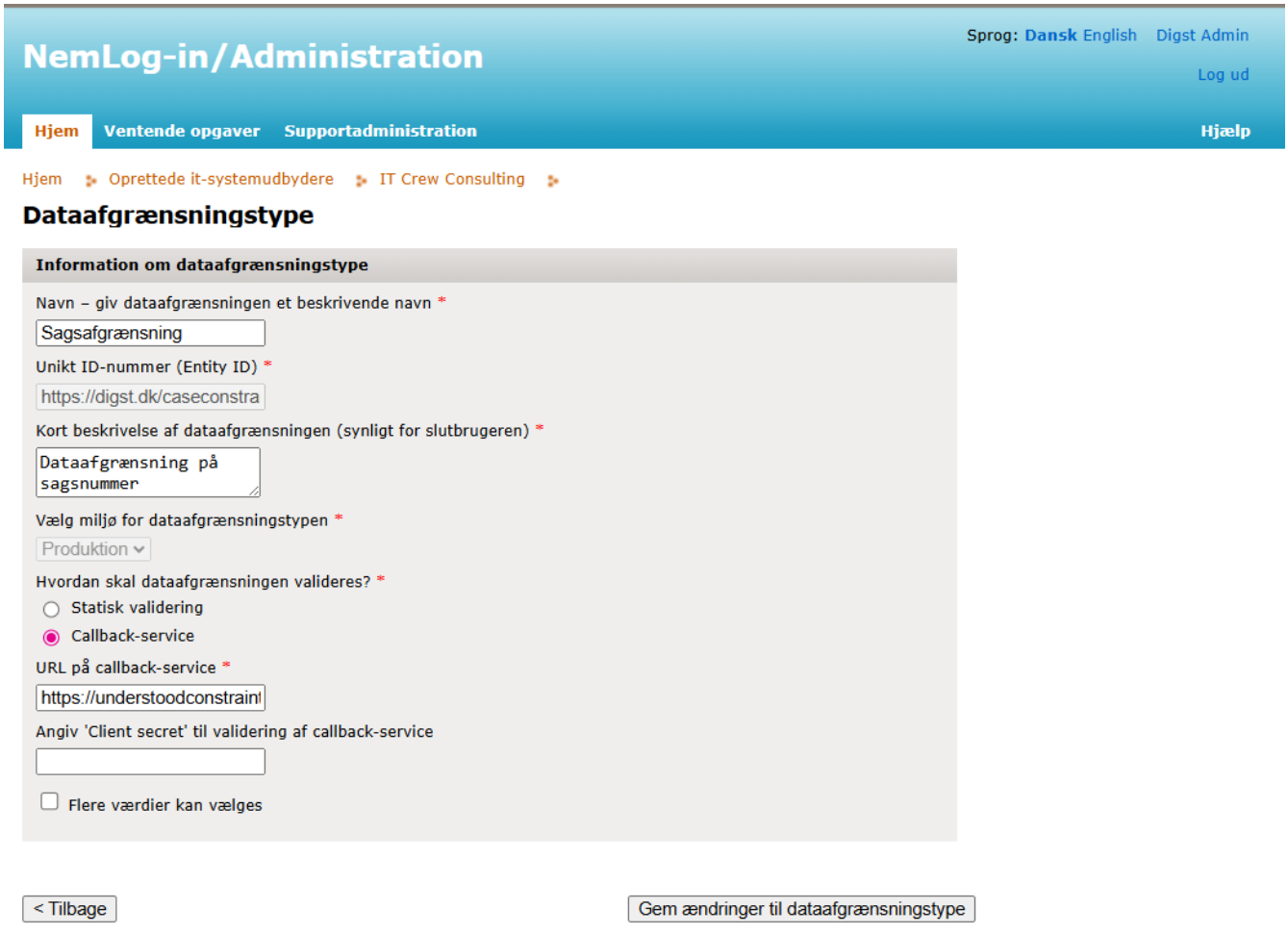
Opret dataafgrænsning med callback validering

Ansvarlig: Administrator for it-systemudbyder

Som administrator for it-systemudbyderen skal du initiere oprettelsen af dataafgrænsningen. Sikrer derfor:

1. Et beskrivende navn for dataafgrænsningen efterfuldt af et unikt ID-nummer (EntityID).
2. En kort beskrivelse af dataafgrænsningen. Vær opmærksom på at denne beskrivelse er synlig for slutbrugeren.
3. Valg af miljø samt valideringsmetode og indsæt URL på callback-servicen. Vær opmærksom på at denne URL skal whitelistes. Læs mere herom i [Whitelist constraint callback] [WL].
4. Såfremt ønsket, at angive en Client Secret til validering af callback-servicen.
5. Ændringerne gemmes.

Se eksempel på en udfyldt dataafgrænsningstype med callback validering nedenfor:

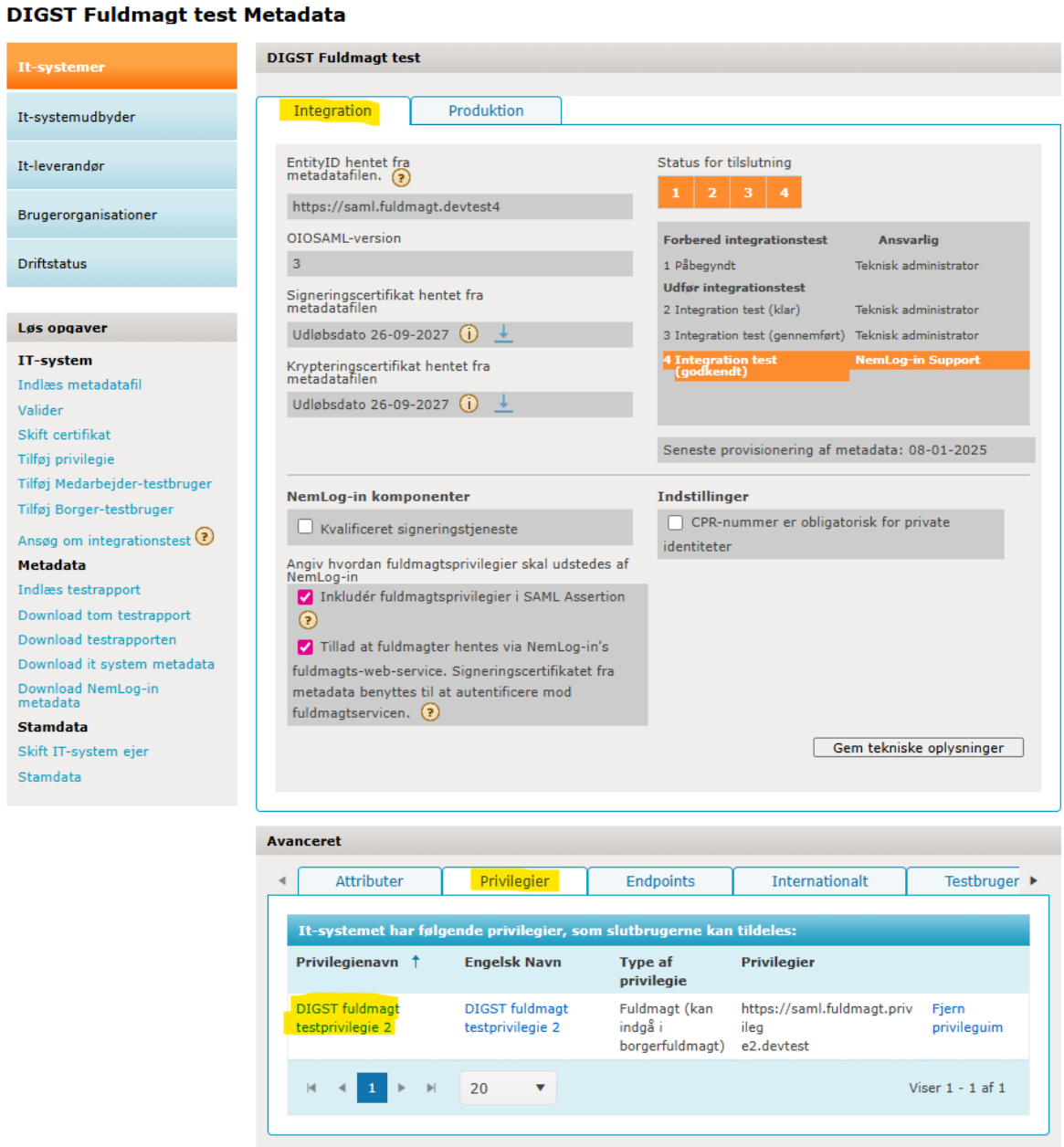


Tilknyt dataafgrænsning til systemer som allerede har et privilegie

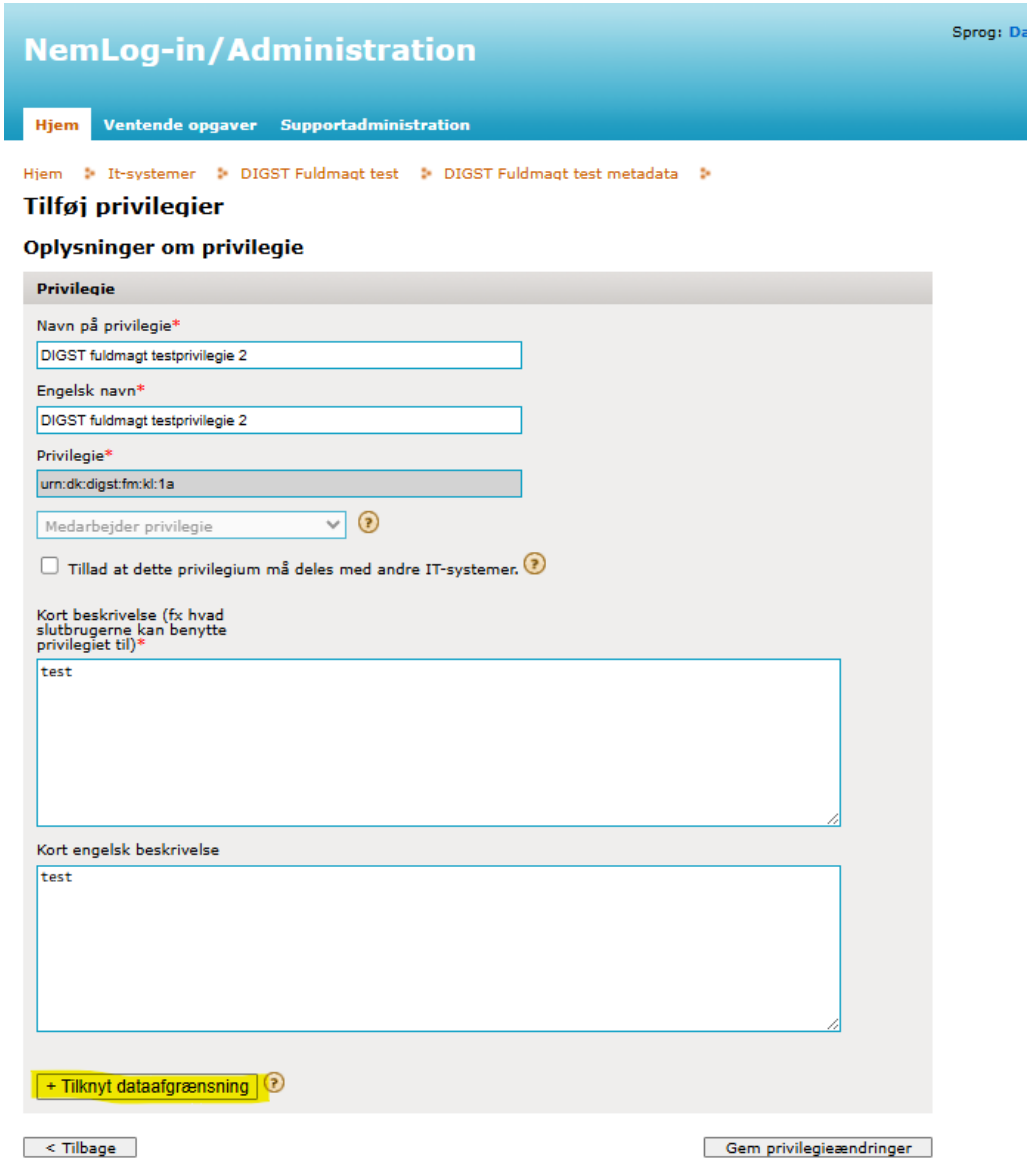
Ansvarlig: Teknisk administrator for it-systemet

Teknisk administrator skal i NemLog-in Administration finde det relevante it-system og det privilegie, som dataafgrænsningen ønskes tilknyttet. Vær opmærksom på at dataafgrænsningen skal tilknyttes privilegiet i integrationstest-fanen.

1. Tryk på det ønskede privilegie.



2. Vælg ”Tilknyt dataafgrænsning” i bunden. Herefter er det muligt at tilknytte en dataafgrænsning.



OBS: Der skal oprettes en ny version af privilegiet, hvis der senere foretages rettelser. Det er vigtigt at kontakte Digitaliseringsstyrelsen efter tilføjelse af en dataafgrænsning til et eksisterende privilegie i Integrationstestmiljøet, således det sikres, at beskrivelser og evt. krav om dataformat er tilpasset den øvrige anbefalende kommunikationsstil til slutbrugere. Henvendelsen skal ske inden der provisionernes til Produktion. Skriv hvilket it-system og hvilket privilegie, dataafgrænsningen omhandler.

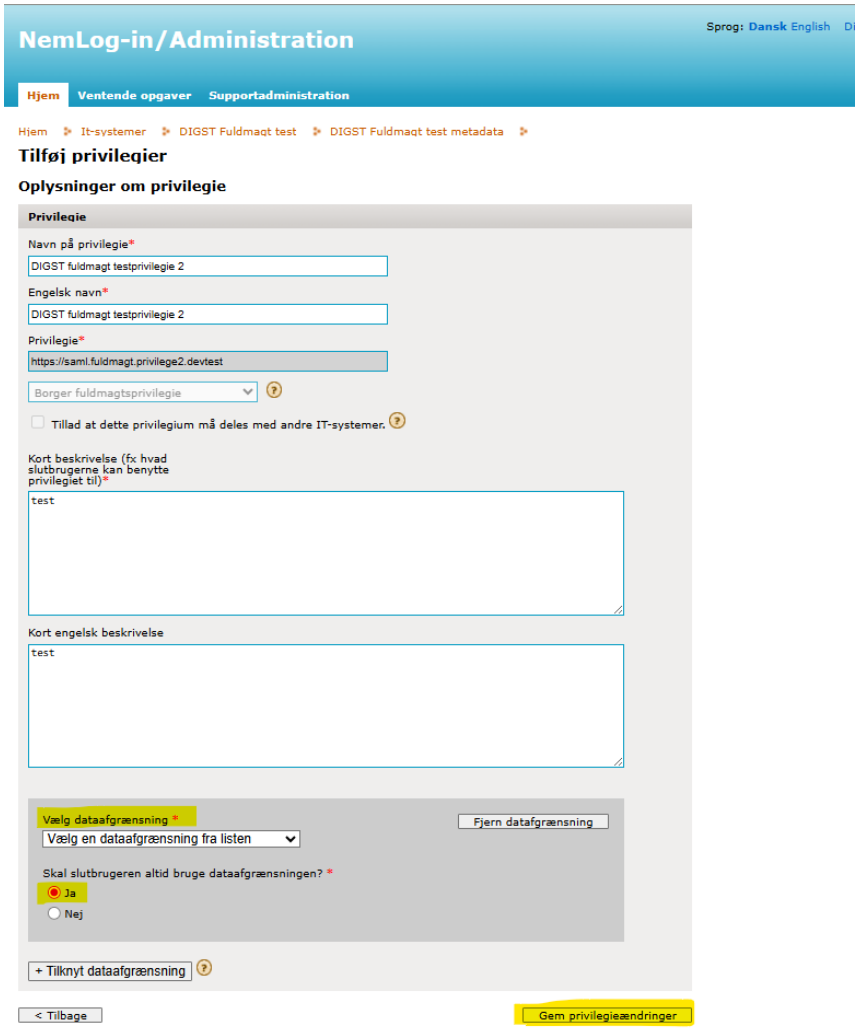
For rettigheder/erhvervsfuldmagter i MitID Erhverv kontakt:

mitiderhverv@digst.dk

For borgerprivilegier kontakt Digital Fuldmagt Forvaltningen på:

digitalfuldmagt@digst.dk

3. Vælg den ønskede dataafgrænsning.



4. Vælg om slutbrugeren altid skal bruge dataafgrænsningen. For borgerfuldmagter er det vigtigt, at der vælges nej, således dataafgrænsningen bliver et frivillig valgt for borgeren, hvilket muliggør de analoge arbejdsgange, hvor fuldmagtsanmodningen sendes via fysisk brev fx hvis fuldmagtsgiver er digitalt udfordret.
5. Gem privilegieændringerne.

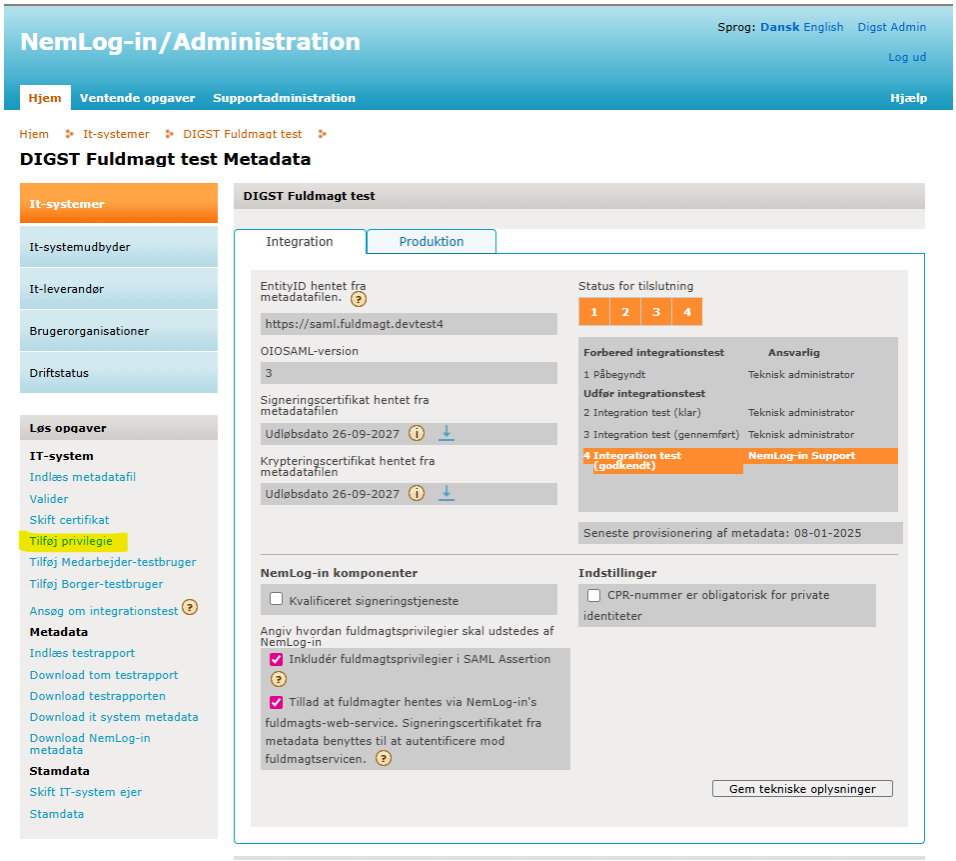
Tilknyt dataafgrænsning til systemer som ikke har privilegier

Ansvarlig: Teknisk administrator for it-systemet

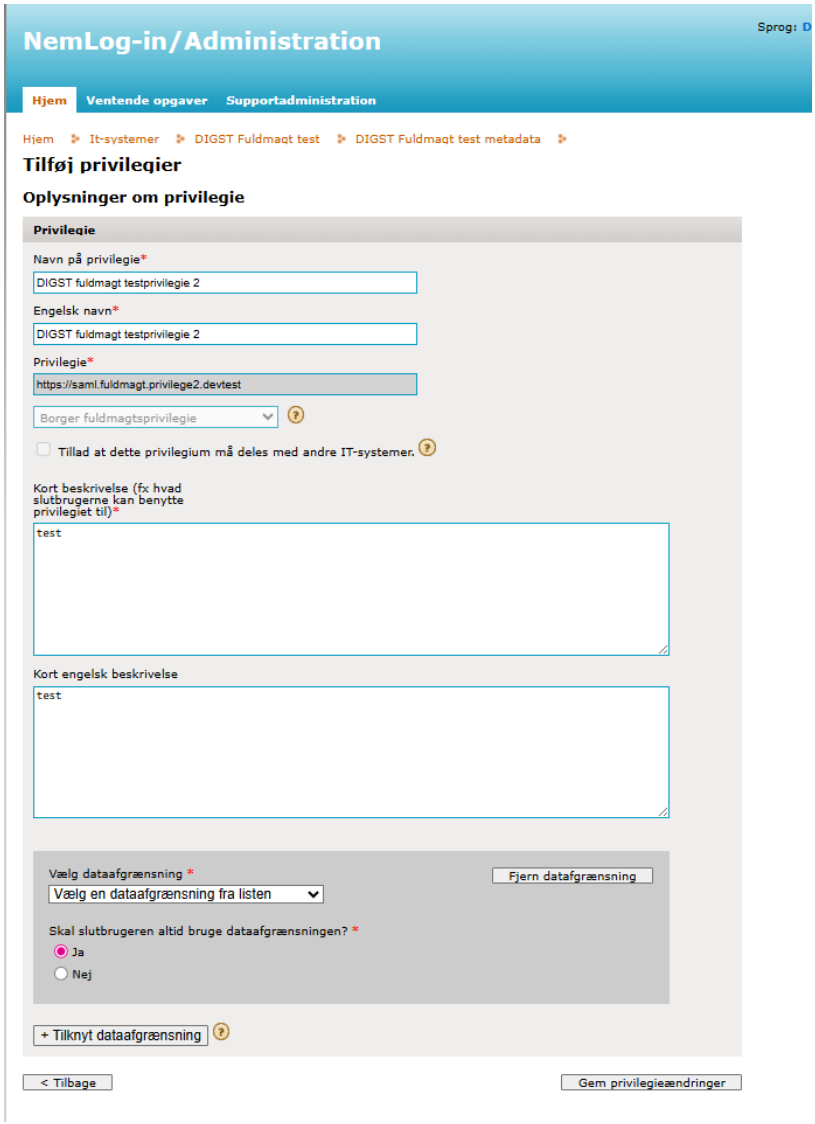
1. Find det relevante it-system og tilføj et privilegie i venstresiden. Vær opmærksom på at dette foretages i integrationstest-fanen.

   Læs hvordan privilegier oprettes i Brugermanualen til NemLog-in Administration ved tvivl herom:

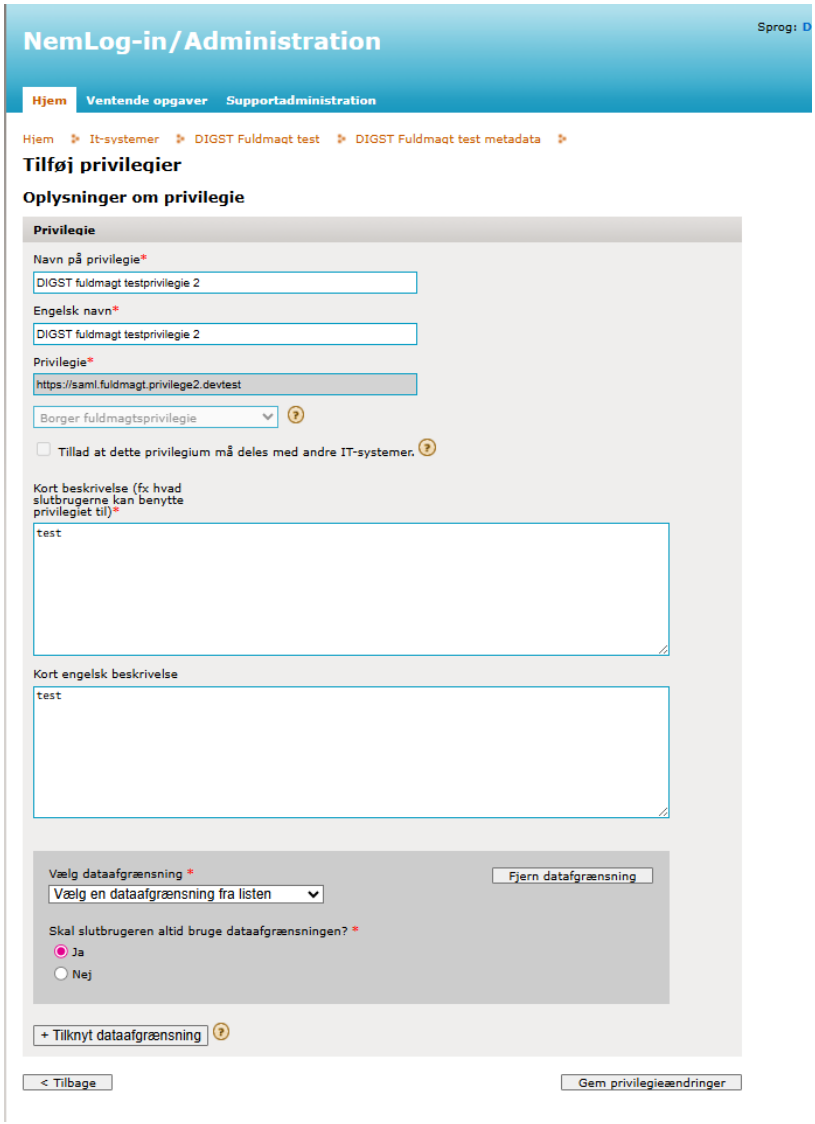
   https://cms.nemlog-in.dk/media/slibbjiv/brugermanual-til-nemlog-in-administration.pdf



2. Når de relevante oplysninger om privilegiet er udfyldt, vælg Tilknyt dataafgrænsning.



3. Vælg den ønskede dataafgrænsning.
4. Vælg om slutbrugeren altid skal bruge dataafgrænsningen. For borgerfuldmagter er det vigtigt, at der vælges nej, således dataafgrænsningen bliver et frivillig valgt for borgeren, hvilket muliggør de analoge arbejdsgange, hvor fuldmagtsanmodningen sendes via fysisk brev fx hvis fuldmagtsgiver er digitalt udfordret.



5. Gem privilegieændringerne.

5.4. Whitelisting af ip-adresser ifm. callback validering i test og produktion

Det er nødvendigt, at der foretages konfiguration i firewalls i forbindelse med opsætning af it-systemudbyderens callback service:

- NemLog-ins firewall skal konfigureres til at tillade udgående kald mod it-systemudbyderens callback service (ip-adresse).
- It-systemudbyderens firewall skal konfigureres til at tillade indgående kald fra NemLog-in til callback servicen. NemLog-in public IP (152.73.246.250).

For at få åbnet for NemLog-ins firewall skal blanketten "Whitelisting af IP-adresser" udfyldes.

https://blanket.virk.dk/blanketafvikler/orbeon/fr/nem_v/85_2e113de92b0e192acbbcd870d99ced0c15c39a80/new?fr-language=da

Der skal indsendes én blanket pr. Whitelisting (URL+IP-adresse – altså én pr. it-systemudbyderens miljø.)

Bemærk, at det kræver MitID Erhverv at udfylde blanketten.

Når whitelisting er gennemført, får I en e-mail fra os.

5.5. Vigtige tips og tricks

Hvis callback-servicen ikke fungerer, kan det være relevant at gennemgå nedenstående tjekliste:

- Modtages der et HTTP kald fra NemLog-in? Hvis ikke, så tjek, at der er åbnet for de korrekte IP-adresser i begge firewalls.
- Kan callback-servicen validere client secret og TLS-klientcertifikat fra NemLog-in korrekt, eller afvises kaldet i adgangskontrollen?
- Modtager callback-servicen de inputparametre, som forventes (constraint EntityID, system ID, privilegename, scope m.m.), og har parametrene de forventede værdier?
- Afsendes der et http-svar fra it-systemudbyderens callback-service?
- Er svaret korrekt formateret som JSON-liste med key/value pairs som vist i billedet nedenfor?

```
"ConstraintValueData": {
    "type": "object",
    "properties": {
        "ConstraintValueUuid": {
            "format": "uuid",
            "type": "string",
            "example": "0ae1a44b-e7c0-470f-8c47-568b5dd06887"
        },
        "ConstraintValueDescription": {
            "type": "string"
        }
    }
}
```

Hvis ovenstående tips og tricks er forsøgt og callback validering fortsat fejler, kan der rettes henvendelse til Digitaliseringsstyrelsen til:

nemlogin@digst.dk

Følgende oplysninger skal inkluderes, således Digitaliseringsstyrelsen kan diagnosticere problemet:

- CVR-nummer på den it-systemudbyder, som forsøger at anvende callback-validering ifm. dataafgrænsninger
- Beskrivelse af problemet, herunder hvad der er forsøgt, hvilket miljø der opereres på m.m.

Type af oplysninger	Beskrivelse
Emne	Fejl i callback-service – [it-systemnavn] – [miljø]
Oplysninger it-systemet	• Navn på it-system • Entity-ID • Miljø • Callback endpoint (URL) • Kontaktperson
Tidspunkt for fejl	• Dato og tidspunkt • Eventuelt request-ID / correlation-ID
Fejlbeskrivelse	• Kort beskrivelse af problemet, fx: Callback fra NemLog-in modtages ikke / modtages men fejler i validering / returnerer fejl.
Observeret adfærd	• HTTP request modtaget: (ja/nej) • HTTP statuskode returneret • Eventuel fejlmeddelelse

Type af oplysninger	Beskrivelse
Eksempel på request/response (hvis muligt)	• Request (headers/body) • Response (statuskode/body)
Loguddrag	• Relevant loguddrag fra tidspunktet for fejlen.
Netværk og adgang	• DIGST IP-adresser åbnet i firewall: (ja/nej) • TLS-klientcertifikat installeret og gyldigt: (ja/nej)
Reproducerbarhed	• Opstår fejlen hver gang eller sporadisk? • Trin til at genskabe fejlen (hvis muligt)