Brugervejledning til Administrationsmodulet for leverandører

Fælleskommunalt Administrationsmodul

Udarbejdet for:

KOMBIT A/S

Halfdansgade 8

2300 København S

Revision: 1.128
November 2026

Indhold

Changelog 4

1 Indledning 10

2 Funktionalitet i Fælleskommunalt Administrationsmodul 10

3 Begreber 10

4 Tværgående elementer i menuer 15

4.1 Venstremenu i Administrationsmodulet 15

4.2 Generel funktionalitet 16

4.3 Søgekriterier huskes 17

5 Arbejdsgange i Administrationsmodulet 18

5.4 Oprettelse af organisation 18

5.5 Log på Administrationsmodulet 18

5.6 Opgaveoversigt 21

5.7 Tilslut it-system 24

5.4.1 Stamdata 25

5.4.2 Dataafgrænsningstyper 28

5.4.3 Anvendersystem 30

5.4.4 Brugervendt system 32

5.4.5 Identity Provider 41

5.4.6 Serviceudbyder 43

5.8 Rediger it-system 52

5.9 Slet it-system 60

5.10 Skift af certifikat 62

5.7.1 Anvendersystem 62

5.7.2 Brugervendt System 62

5.7.3 Service Udbyder 63

5.11 Anmod om en serviceaftale 64

5.8.1 Klassisk fremgangsmåde 64

5.8.2 Anmodning ved brug af Integrationer 71

5.12 Vis serviceaftaler 79

5.13 Vis integrationer 82

5.14 Serviceaftaleoverblik (beta) ... 83
5.15 Kopier serviceaftaler ... 89
5.16 Tilbagekald serviceaftale ... 92
5.17 Opsig serviceaftale ... 93
5.18 Anmod om føderationsaftale ... 94
5.19 Vis føderationsaftale ... 97
5.20 Opsig føderationsaftale ... 98
5.21 Vis, rediger eller slet en organisation ... 100
5.22 Rapporter ... 102
5.23 Brugerprofil ... 112
5.24 Adviseringer ... 116
6 Testmuligheder som Myndighed ... 120
6.1 Test med støttesystemet Organisation ... 120
6.2 Test af adgangsstyring for brugere ... 120
6.3 Test af adgangsstyring for systemer ... 121
6.4 Sådan bliver du myndighed i testmiljøet ... 121
6.5 Vilkår for leverandører der agerer myndighed i testmiljøet ... 122
7 Kontakt og Support ... 122

KOMBIT

Changelog

Date	Change	Responsible	Revision
14-02-2018	Release 3. Changelog er tilføjet Kopier serviceaftale er tilføjet Føderationsaftaler er tilføjet Rapporter er tilføjet Brugerprofil er tilføjet Adviseringer er tilføjet	KFN	X
22-03-2019	Indarbejdet vejledning til Serviceplatformens administrationsmodul for leverandører. Indarbejdet vejledning til, hvordan leverandører kan blive oprettet med rollen myndighed, så leverandøren kan agere myndighed i testmiljøet	COR	
02-05-2019	CCR0453: Opdateret beskrivelse af redigering af systemspecifikke dataafgrænsningstyper og kopiering af serviceaftaler	SMAH	1.36
07-05-2019	CCR0471: Opdateret ”Opgaveoversigt” afsnit med ny dialog og refereret til dette i ”Rediger it-system” og ”Vis, rediger eller slet en organisation”.	ALO	1.45
13-05-2019	CCR0485: Tilføjet information om servicetypen ”Filservice med rutning” samt dens indflydelse på opret service, opret service aftale, servicekoblinger og service grupper.	Guest-CCBC	1.46
14-05-2019	Opdateret generel funktionalitet afsnit med obligatorisk felt markering.	SNN	1.47
15-05-2019	CCR0485: Begreb: tilføjet summary til ny servicetype Filservice med rutning	Guest-CCBC	1.48
15-05-2019	Ændret revision og changelog efter KOMBITS ønsker	Guest-CCBC	1.49
21-05-2019	Indarbejdet vejledning til ”Skift af certifikat”.	XKHI	1.50

04-06-2019	Godkendt af KOMBIT og renset for ændringsmarkeringer.	MATGS	1.52
27-06-2019	CCR0489: Tilføjet beskrivelse af ny funktionalitet til sletning af brugersystemroller, der er i brug på jobfunktionsroller.	AKK	1.54
04-07-2019	Godkendt af KOMBIT og renset for ændringsmarkeringer.	AKK	1.55
04-07-2019	CCR0472: Tilføjet beskrivelse af ny funktionalitet til oprettelse/redigering/sletning af callback endpoints på anvendersystem. Ændret og tilføjet beskrivelse af serviceparametre på anmod om serviceaftale.	Guest-CCBC	1.56
25-07-2019	Godkendt af KOMBIT og renset for ændringsmarkeringer.	MATGS	1.60
05-08-2019	CCR0499: Tilføjet Step Up og Scoping til Identity Provider.	SMAH	1.62
27-08-2019	Afsnit 5.8 opdateret for at afspejle retningslinjer for oprettelse og godkendelse af serviceaftaler.	XJPK	1.65
20-11-2019	CCR0501: Vejledning for rapporten "Brugersystemroller" tilføjet. CCR0499: Step-up og Scoping er taget ud som følge af, at CCR0499 er udgået af release SP2019-11.	LBS	1.68
21-11-2019	Godkendt af KOMBIT og renset for ændringsmarkeringer.	MATGS	1.69
04-02-2020	Merge af CCR0499 rettelser ind i version til SP2019-11. Afsnit 5.4.5.	HSC	1.71
30-03-2020	CCR0510: - Arkiv/Arkiver begreb tilføjet. Afsnit 3 - Opdateret vejledning ved visning af serviceaftaler. Afsnit 5.8 5.9 og 5.11 - Opdateret vejledning ved sletning af IT-system. Afsnit 5.6 - Opdateret vejledning omkring udløb af aftaler. Afsnit 5.11	GUEST-CCBC	1.76

	- tilføjet flere adviseringer. Afsnit 5.18		
11-05-2020	CCR0526: - Opdateret screen dump. Afsnit 5.8 - Tilføjet beskrivende tekst til tilføjet info ikon Afsnit 5.8	GUEST-CCBC	1.78
18-05-2020	CCR0509: - Tilføjet afsnit som beskriver genindlæsning af søgekriterier. Afsnit 4.3	MATGS	1.79
04-06-2020	CCR0512: - Opdateret beskrivelse af brugerprofil til også at omhandle setup af adviseringer, afsnit 5.17 - Opdateret beskrivelse omkring adviseringer til at matche det nye setup hvor man kan lave til og fravalg af disse, afsnit 5.18	OLL	1.83
14-08-2020	CCR0533: - Opdateret serviceaftale navne validering Afsnit 5.8 - Tilføjet bemærk omkring mulighed for åbning af serviceaftale med Ctrl og Shift klik Afsnit 5.9	GUEST-CCBC	1.89
08-09-2020	CCR0531: - Tilføjet nyt afsnit Tilbagekald Serviceaftale - Opdateret Table of Content - Små rettelser til fejl fra tidligere opgaver	GUEST-CCBC	1.90
09-09-2020	CCR0530 - Rettet afsnit om rapporter	OLL	1.94
23-09-2020	CCR0530 - Rettet i afsnit omkring rapporten ”Services og aftaler”	OLL	1.99
23-09-2020	CCR0532 - Rettet i vejledning til oprettelse af dataafgrænsningstyper og anmodning om serviceaftale	MATGS	1.100
14-10-2020	CCR0528 - Tilføjelse af Attributprofil og NSIS sikringsniveau til identity provider og Brugervendt system. - 5.4.4 Brugervendt system - 5.4.5 Identity Provider	LBS	1.103

08-07-2021	CCR0541: Beskrivelse af konfiguration af brugervendte systemer og identity providere til Context Handler NSIS CCR0542: Beskrivelse af ny certifikatrapport	MATGS	1.107
12-09-2022	Konsolideret version: - CR117: Context Handler NSIS (SSE CCR541, CCR542) - CR134: ADM2.0 Fase 1 (SSEs version 1.102 leveret med CCR0546 flettet ind) - CR074: NemLog-in3	MATGS / SUH / HKV	1.108
07-10-2022	Opdateret efter KOMBITs review.	HKV	1.109
17-11-2022	Konsolideret version: CR073: Opdatering af OCES certifikatpolitik v7 under sektion 3 CR155: Opdateret SP_Admin login screen under sektion 5.2 CR187: Opdateret 5.4.4 Krævet NIST assurance level samt nyt screenshot	Lal / Sidney	1.110
29-11-2022	Opdateret efter under review	HKV	1.111
07-12-2022	Alle ændringer for CR073, CR155 og CR187 er accepteret af KOMBIT. Dokument ophøjes til v1.112	Anqi Huang	1.112
31-01-2022	Alle ændringer for CR190 er accepteret af KOMBIT. Dokumentet ophøjes til v.1.113	Thomas Ebsen	1.113
07-02-2023	Alle ændringer for CR198 er godtaget af KOMBIT. Dokumentet ophøjes til v.1.114	Thomas Ebsen	1.114
08-12-2023	CR260 introducerer mulighed for at redigere visse OIOSAML-egenskaber for IdP'er i det eksterne testmiljø. Afsnit 5.4.5 opdateret, så dette afspejles Alle ændringer for CR260 er godkendt af KOMBIT. Dokumentet ophøjes til v.115	Henrik Vosegaard	1.115
08-03-2024	CR135 introducerer anmodningsflow for serviceaftaler baseret på Integrationer	Henrik Vosegaard	1.115 CR135_v1
26-04-2024	Opdateret efter KOMBITs review	Henrik Vosegaard	1.115 CR135_v2
06-05-2024	Alle ændringer for CR135 er godkendt af KOMBIT. Dokument ophøjes til v. 1.116	Anqi Huang	1.116

17-05-2024	Ændringer til visning af serviceaftaler via Integrationer, CR230	Henrik Vosegaard	1.116 CR230_v1
10-06-2024	Mindre opdateringer efter KOMBITs review	Henrik Vosegaard	1.116 CR230_v2
24-06-2024	Mindre opdateringer efter KOMBITs review	Henrik Vosegaard	1.116 CR230_v3
28-06-2024	Alle ændringer for CR230 er godkendt af KOMBIT. Dokument ophøjes til v. 1.117	Anqi Huang	1.117
19-08-2024	CR287: Ændring af OIOSAML Profiler-værdier i afsnit 5.4.5 og 5.5	Henrik Vosegaard	1.117 CR287_v1
05-09-2024	Alle ændringer for CR287 er godkendt af KOMBIT- Dokument ophøjes til v. 1.118	Anqi Huang	1.118
16-09-2024	Punkt OIOSAML profiler på side 37 er opdateret med fremsendt formulering fra KOMBIT.	Anqi Huang	1.119
09-05-2025	CR298: Opdateret, så administration af Brugervendt System og IdP afspejler, at STS1 og CH1 er blevet udfaset	Henrik Vosegaard	1.119 CR298_v1
25-06-2025	CR298: Mindre opdateringer efter review	Henrik Vosegaard	1.119 CR298_v2
27-06-2025	Alle ændringer for CR298 er godkendt af KOMBIT. Dokument ophøjes til v. 1.120	Nicklas Preisler Petersen	1.120
18-08-2025	Ændringer ifht. CR304 og CR312	Henrik Vosegaard	1.120_CR304v2
19-09-2025	Alle ændringer for CR304 og CR312 er godkendt af KOMBIT. Dokument ophøjes til 1.121	Nicklas Preisler Petersen	1.121
18-11-2025	Nyt menupunkt: Serviceaftaleoverblik	Henrik Vosegaard	1.121_ADO5548 v1
15-01-2026	Beskrivelse af fanen Serviceaftaleoverblik > Anvender	Henrik Vosegaard	1.121_ADO5548 v1 ADO5550 v1
22-01-2026	Alle opdateringer for ADO5548 er accepteret af KOMBIT. Merged dokumentet sammen med opdateringerne fra CR263 som blev godkendt i version 1.121. Dokument ophøjes til v1.122.	Nicklas Preisler Petersen	1.122
27-02-2026	Alle opdateringer for ADO5550 er accepteret af KOMBIT. Merged dokumentet med hoveddokumentet. Dokument ophøjes til v.1.123.	Nicklas Preisler Petersen	1.123
27-02-2026	ADO9594: Ekstra kontaktoplysninger for it-system ADO11961: Anmod-knap i Serviceaftaleoverblik	Henrik Vosegaard	1.123_ADO9594 _ADO11961_v1
23-03-2026	ADO9594 + ADO11961: Rettelser efter review	Henrik Vosegaard	1.123 ADO9594 _ADO11961_v2

24-03-2026	Serviceaftaleoverblik: - ADO12554 Valg af tabelkolonner tilføjet - ADO12546 Oprettelsesdato tilføjet - ADO12550 Rækkefølge af faneblade	Henrik Vosegaard	1.123 ADO9594 _ADO11961_v2 ADO12554 _ADO12546 _ADO12550_v1
28-03-2026	Alle opdateringer for ADO9594, ADO11961, ADO12546, ADO12550 og ADO12554 er accepteret af KOMBIT. Dokument ophøjes til v. 1.124	Nicklas Preisler Petersen	1.124
08-05-2026	KOMBIT-7743: Skærmbillede opdateret	Henrik Vosegaard	1.124_KOMBIT-7743v1
27-05-2026	Alle opdateringer for INCEU20544201 er accpeteret af KOMBIT. Dokument ophøjes til v. 1.125	Nicklas Preisler Petersen	1.125
09-07-2026	ADO10161: Tilføjet OIDC-understøttelse for Brugervendte Systemer	Henrik Vosegaard	1.125 ADO10161_v1
13-08-2026	Alle opdateringer for ADO10161 er accepteret af KOMBIT. Dokument ophøjes til v.1.126	Nicklas Preisler Petersen	1.126
28-09-2026	ADO5703: Serviceaftaleoverblik for Udbyder	Henrik Vosegaard	1.126 ADO5703v1
28-09-2026	ADO10031: Validering af SAML Metadata	Henrik Vosegaard	1.126 ADO10031v1
01-10-2026	ADO10248: Filservices og webservices i samme serviceaftale	Henrik Vosegaard	1.126 _ADO10248v1
14-10-2026	Alle opdateringer for ADO5703, ADO10031 og ADO10248 er accepteret af KOMBIT. Dokument ophøjes til v. 1.127	Nicklas Preisler Petersen	1.127
21-10-2026	ADM-13433: Kolonnevalg huskes ADM-21658: Bootstrap token ADM-20502: Roller i brugerprofil-overblik	Henrik Vosegaard	1.127 _ADM13433 &21658 &20502v1
03-11-2026	Skærmbillede opdateret efter review	Henrik Vosegaard	1.127 _ADM13433 &21658 &20502v2
05-11-2026	Alle opdateringer for ADM13433, ADM21658 og ADM20502 er accepteret af Kombit. Dokument ophøjes til v. 1.128	Nicklas Preisler Petersen	1.128

1 Indledning

Denne vejledning beskriver de arbejdsgange og den funktionalitet som understøttes af Fælleskommunalt Administrationsmodul i forhold til dig som leverandør af it-løsninger, der skal anvende den fælleskommunale infrastruktur.

Formålet med Administrationsmodulet er at understøtte samarbejdet mellem myndigheder og it-leverandører i de arbejdsgange, der involverer aftaler og styring af roller, adgang til services, systemer og data. Langt størsteparten af funktionaliteten understøttes af Fælleskommunalt Administrationsmodul.

2 Funktionalitet i Fælleskommunalt Administrationsmodul

I **Fælleskommunalt Administrationsmodul** håndteres al funktionalitet vedrørende adgangsstyring:

- Oprettelse af it-systemer
    - Anvendersystemer
    - Brugervendte systemer
    - Identity Provider
    - Serviceudbyder
- Serviceaftaler
- Føderationsaftaler

3 Begreber

I denne brugervejledning optræder en række begreber, som du kan læse betydningen af herunder, og som er relevante i forhold til it-leverandørernes brug af Administrationsmodulet.

Anvendersystem	Et it-system der anvender en service, og hvor aftaler om adgang til servicen styres via serviceaftaler i Administrationsmodulet.
Arkiv/Arkiveret	Serviceaftaler og føderationsaftaler vil i nogle tilfælde blive arkiveret. Dette betyder, at den pågældende aftale fjernes, ikke længere er aktiv og en kopi af aftalen lægges i en arkivtabel til historisk visning.
Assurance level	I Administrationsmodulet bruges der henholdsvis ”Krævet assurance level” og ”Udbudt assurance level”, som man skal forholde sig til i forbindelse med oprettelsen af et nyt it-system. Krævet assurance level: Angiver det krævede niveau af tillid til den identitet, der er i de tokens, som modtages af det brugervendte system. Dette skal angives i henhold til [OIO-A-LEVEL]. Udbudt assurance level: Angiver den udbudte grad af tillid til den identitet, der er i de tokens, som Identity Provideren udsteder. Dette skal angives i henhold til [OIO-A-Level].

Attributprofil	Attributprofilen er en specifik type af attribut, der bruges i burgervendte systemer. Da forskellige systemer kan have brug for forskellige attributter, udpeger systemet en attributprofil, som kan tilpasses til det specifikke system. Ændring af attributprofilen er kun tilladt for KOMBIT, og som standard benytter systemet den fælleskommunale profil. Du kan læse mere om attributprofil i dokumentet **" Vejledning til Adgangsstyring for brugere"** via dette link.
Bruger	En person der anvender Administrationsmodulet via en tilknyttet administrationsrolle i NEMLOG-IN.
Brugersystemrolle	Gruppering af rettigheder, der definerer adgang og adgangsbegrænsninger til et specifikt Brugervendt system.
Brugervendt system	Et it-system der udstiller en sikret og adgangsbeskyttet brugergrænseflade, der tilgås via en browser.
Certifikat	Der er to typer certifikater, du kan bruge i din organisation: - Et **organisationscertifikat** er et certifikat, som du bruger til at repræsentere din organisation. Der er ingen personnavne i certifikatet og certifikatet indeholder typisk kun organisationens navn, CVR-nummer og en e-mailadresse. - Et **systemcertifikat** er en specialisering af organisationscertifikatet. Systemcertifikatet repræsenterer et specifikt system i din organisation. Certifikatet udstedes til og bruges af systemet til at identificere systemet over for andre systemer og kryptere trafikken mellem systemerne.
Certifikatudløb	Et certifikat har en gyldighedsperiode indeholdende en start- og en slutdato. Hvis dags dato er større end et certifikats slutdato, så er certifikatet udløbet og ikke længere gyldigt.
Dataafgrænsning	Afgrænsning på en systemrolle, som indsnævrer systemrollens virkefelt.
Dataafgrænsningstype	Ved tilknytningen af en servicesystemrolle til en service eller en brugersystemrolle til en jobfunktionsrolle, er det muligt at tilknytte én eller flere dataafgrænsninger, som angiver hvilke forretningsobjekter eller attributter, systemrollen kan anvendes på. Dette forudsætter dog, at det underliggende it-system understøtter den specifikke dataafgrænsning.
Dataejer	Den myndighed der ejer data indenfor et givent område.
Datamodtager	Den myndighed der ønsker at behandle de modtagne data inden for et givent område. Det kan både være en myndighed eller en leverandør.
Forretningsområde	Logisk entitet til gruppering af integrationer under den samme begrebs- og informationsmodel. Eksempler er: Person, Kontanthjælp og Sundhed.

Føderationsaftale	En føderationsaftale giver en Identity Provider ret til at udstede tokens, der bevidner, at brugere er autentificeret i kontekst af den myndighed, der har godkendt aftalen. Dette token anvendes til at afgøre, hvorvidt en given bruger får adgang til et Brugervendt system på vegne af en given myndighed.
Identity Provider	System der udsteder tokens vedrørende brugeres identitet, egenskaber og roller.
Integration	En dataudveksling mellem it-systemer via en eller flere services, som giver en samlet forretningsmæssig værdi.
Integrationsversion	Udtrykker en bestemt version af en integration, som deler forretningsmæssig hensigt med andre versioner af integrationen.
It-leverandør	I Administrationsmodulet er en it-leverandør den part, der tilslutter systemer og initierer alle aftaler, der vedrører it-systemet.
It-system	It-system i Administrationsmodulet er instansen af et it-system, dvs. den specifikke installation af it-systemet. Det kunne eksempelvis være et fagsystem så som Kommunernes Ydelsessystem. Hvis it-systemet er registreret i både et test og et produktionsmiljø vil det fremgå som to forskellige instanser.
Jobfunktionsroller	Gruppering af brugersystemroller for en myndighed, der anvendes ved tildeling af brugeradgange hos myndigheden.
Medarbejdercertifikat	En elektronisk attest, som angiver certifikatindehaverens offentlige nøgle sammen med supplerende information, og som entydigt knytter den offentlige nøgle til identifikation af certifikatindehaveren. Et medarbejdercertifikat er udstedt til en ansat i en organisation.
Myndighed	Myndighed er i Administrationsmodulet den organisation, der godkender anvendelsen af services i forhold til et anvendersystem. En myndighed kan eksempelvis være kommuner, stat eller Udbetaling Danmark (UDK).
Organisation	En organisation anvender Administrationsmodulet for indgåelse og administration af aftaler samt administration af it-systemer.
Post-config-URL	Serviceudbyderen kan tilføje en post-config-URL, hvis der er behov for, at de myndigheder hvis data, der er udbudt af en given service, laver yderligere konfigurationer, inden den udbudte services kan tages i brug.
Pre-config-URL	Serviceudbyderen kan tilføje en pre-config-URL, hvis der er behov for, at leverandøren af anvendersystemet laver yderligere konfigurationer, inden den udbudte service kan tages i brug.
SAML metadataudløb	SAML metadata har en gyldighedsperiode indeholdende en start- og en slutdato. Hvis dags dato er større end et slutdatoen i SAML metadatafilen, så er det udløbet og ikke længere gyldigt.
Service	En udbudt service fra en serviceudbyder, hvor adgang administreres via Serviceaftaler.
Service (logisk)	En veldefineret funktionalitet stillet til rådighed på et netværksendepunkt.
Serviceaftale	En serviceaftale er en aftale, der indgås mellem it-leverandøren af et anvendersystem og den myndighed, der er ansvarlig for data i en service.

Servicegruppe	Et antal af nært beslægtede services, der er samlet i en logisk gruppe.
Servicekobling	En servicekobling betyder, at to services er koblet til hinanden. Når en koblet service vælges, vil begge services blive tilføjet til serviceaftalen. Flere af de udstillede services i Administrationsmodulet er koblede services, idet Serviceplatformen fungerer som proxy for mange kildesystemer. Servicekoblinger administreres af KOMBIT administratoren for at sikre den nødvendige forretningsmæssige sammenhæng.
ServiceMajorversion	En Servicemajorversion er en udgave af en service. Fælles for alle servicemajorversioner er, at de deler samme forretningsmæssige formål med andre instanser af servicen.
Servicesystemrolle	Gruppering af rettigheder, der definerer adgang og adgangsbegrænsninger til en given service.
Servicetyper	I Administrationsmodulet anvendes nedenstående servicetyper: • Simpel Service / Invocation Context: Er certifikatbaseret og enten har anvendersystemet adgang til hele servicen eller også har det slet ikke adgang (der opereres ikke med myndighedskontekst). • Simpel Filtransport Service: Filtransportservice er baseret på SFTP til udveksling af store datamængder. • Simpel Callback Service: Svarer rent sikkerhedsmæssigt til, en Simpel Service, og anvendes til at pushe data fra kilden til anvendersystemet. • Simpel Fælleskommunal Service / Authority Context: Er certifikatbaseret og et anvendersystem tilgår altid servicen på vegne af en given myndighed. Anvendersystemet har enten adgang til hele servicen (for den specifikke myndighed) eller også har det ikke adgang. • Fælleskommunal Service: Er tokenbaseret og et anvendersystem tilgår altid servicen på vegne af en given myndighed. Desuden begrænses anvendersystemets brug af servicen ud fra systemroller, der tildeles anvendersystemet. • Filservice Med Rutning: Denne Filservice er baseret på SFTP til udveksling af store datamængder. For hver Filservice har Anvendersystemet adgang til at aflevere eller hente filer. Hver Filservice tilknyttes en unik integrationsreference (InfRef) og kan underlægges rutning. Du kan læse mere om servicetyperne i dokumentet **"Programmers Guide - Serviceplatformen"** via dette link.
Serviceudbyder	Et it-system, der udstiller services.

Sikringsniveauer	**NIST** NIST sikringsniveauerne også kendt som Level of Assurance, er en klassificering af i hvor høj grad en bruger skal autentificere sig for at få adgang til et brugervendt system. Der er fire hierarkiske niveauer: • Niveau 1 - anvendes ikke i kommunale løsninger • Niveau 2 - kræver at brugeren er logget på med 1 autentifikationsfaktor • Niveau 3 - kræver at brugeren er logget på med 2 autentifikationsfaktorer • Niveau 4 - kræver at brugeren er logget på med 2 autentifikationsfaktorer, hvor styrken af det Elektroniske Identifikationsmiddel skal være beskyttet mod kopiering og manipulering af angribere med stor Angrebskapacitet Bemærk, at NIST alene ser på styrken af de elektroniske identifikationsmidler modsat NSIS som dækker mere. **NSIS** NSIS sikringsniveauerne, er en klassificering af i hvor høj grad en bruger skal autentificere sig for at få adgang til et brugervendt system. Der er tre hierarkiske niveauer: • Niveau Lav - kræver at brugeren er logget på med 1 autentifikationsfaktor • Niveau Betydelig - kræver at brugeren er logget på med 2 autentifikationsfaktorer • Niveau Høj - kræver at brugeren er logget på med 2 autentifikationsfaktorer, hvor styrken af det Elektroniske Identifikationsmiddel skal være beskyttet mod kopiering og manipulering af angribere med stor Angrebskapacitet Bemærk, at NSIS sætter krav til hele livscyklus for elektroniske identifikationsmidler Læs mere her National Standard for Identiteters Sikringsniveauer (NSIS) (digst.dk) **Faktorer** Autentifikationsfaktor er en faktor, der er personlig for den person der forsøger at logge på. Dvs. andre personer må ikke kunne anvende samme unikke faktorer til at logge på med. • Noget du har »Indehaverbaseret Autentifikationsfaktor« - en autentifikationsfaktor, som Brugeren skal bevise at være i besiddelse af (fx en fysisk enhed)

	• Noget du ved »vidensbaseret autentifikationsfaktor« - en autentifikationsfaktor, som Brugeren skal bevise at have kendskab til (fx et kodeord) • Noget du er »iboende autentifikationsfaktor« - en autentifikationsfaktor, der er baseret på et fysisk træk hos en fysisk person, og som Brugeren skal bevise at have (fx biometri)
Systemaktør	Angiver en navngiven rolle, som en potentiel anvender har i forhold til integration.
Systemrolle	Gruppering af rettigheder der definerer adgang til et givet anvendersystem.
UUID	UniversalUniqueID som er en unik nøgle.

4 Tværgående elementer i menuer

I Administrationsmodulet anvendes der begreber og funktionalitet, som er tværgående for systemet. I dette afsnit gives en kort beskrivelse af de tværgående elementer.

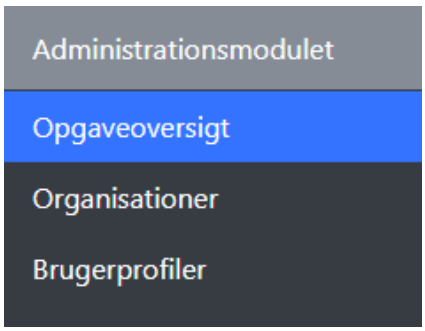
4.1 Venstremenu i Administrationsmodulet

I Administrationsmodulet vises forskellige oversigtspunkter i venstremenuen alt efter, hvilken rolle din bruger har tilknyttet. Har du flere roller, vil du se en kombination af nedenstående eksempler.

Leverandøradministrator: Her vil din venstremenu se ud på følgende måde:



Organisationsadministrator: Her vil din venstremenu se ud på følgende måde:

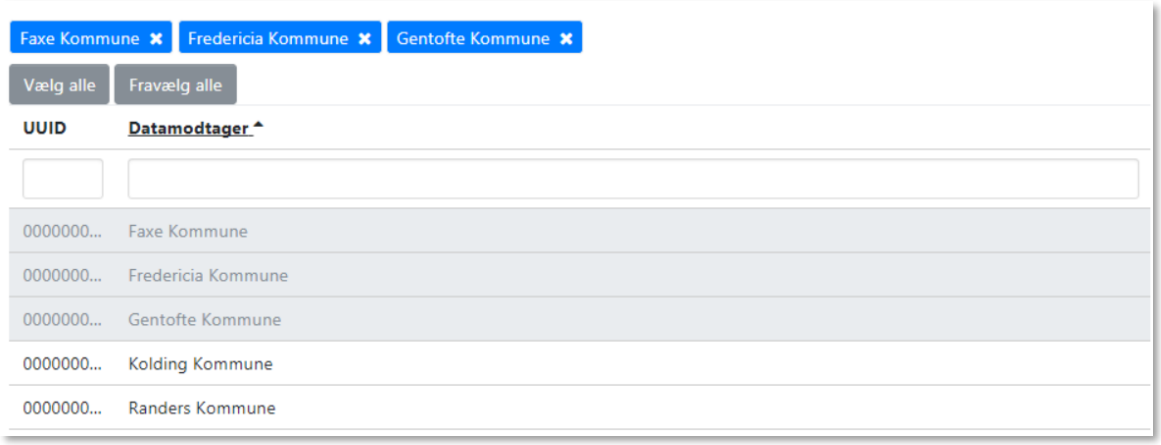


4.2 Generel funktionalitet

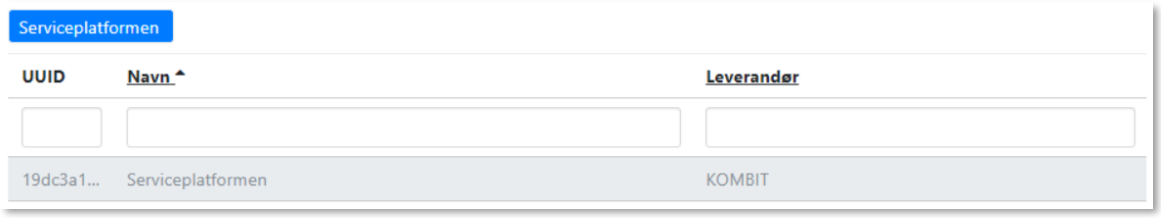
- **Obligatoriske felter**: I Administrationsmodulet er obligatoriske felter markeret med en blå stjerne (*).
- **Annuller**: Hvis du trykker på en "Annuller-knap", forlader du den side, du står på uden at gemme. Herefter kommer du ét trin tilbage, hvilket typisk er tilbage på en oversigtsside.
- **Tilbage**: Hvis du trykker på en "Tilbage-knap", kommer du tilbage til oversigtssiden for den funktionalitet, du netop har været inde på.
- **Slet**: Hvis du trykker på en "Slet-knap", sletter du det indhold, der står på siden, hvor "Slet-knappen" vises. Du vil få en advarselsbesked, som spørger dig, om du er sikker på, at du vil slette indholdet fra Administrationssystemet før det bliver slettet. Efter du har trykket på "Slet", kommer du tilbage på oversigtssiden for det område, du netop var inde på.
- **Hjælpetekster:** På udvalgte felter vil du i Administrationsmodulet kunne se et lille spørgsmålstegn med en cirkel rundt om. Når du klikker på det, får du vist en hjælpetekst, med retningslinjer for, hvordan det pågældende felt skal udfyldes.



- **Flere valg fra liste:** I Administrationsmodulet kan du vælge eksempelvis en række kommuner på en liste. Når du klikker på dem i listen, kommer dine valg op over listen i nogle blå bokse og samtidig bliver dine valg markeret som grå på listen. Klikker du på krydset i den blå boks, fjerner du dit valg på listen. Du kan også fjerne et valg ved at trykke på det i listen, hvor det er blevet markeret som grå. Hvis du trykker på knappen "Vælg alle", vælger du alle fra listen eksempelvis alle kommuner. Trykker du på "Fravælg alle" fjerner du alle de valg, du har gjort.



- **Enkelt valg fra liste:** I Administrationsmodulet skal du vælge eksempelvis et system fra en liste. Når du klikker på et system fra en liste, kommer dit valg op over listen i en blå boks, og samtidig bliver dit valg markeret som grå på listen. Når du kun har mulighed for at vælge én ting fra listen, kommer der ikke noget kryds i den blå boks, hvor den valgte værdi kan slettes. Ønsker du at vælge en anden fra listen, skal du blot vælge fra listen igen, hvorefter dit nye valg erstatter dit tidligere valg.



4.3 Søgekriterier huskes

For nemmere at kunne navigere imellem forskellige elementer og lister, er der implementeret genindlæsning af søgekriterier når brugeren vender tilbage til en liste som tidligere i sessionen er blevet filtreret. Denne funktionalitet gør sig gældende på følgende lister:

- It-systemer
- Serviceaftaler
- Jobfunktionsroller
- Brugerprofiler

Genindlæsningen medfører at filtrering, sortering og sidevalg automatisk bliver påført en liste, der tidligere i samme session har været besøgt af brugeren. Derudover, er der indført en farvemarkering af det senest inspicerede element på de fire lister, således at det er tydeligt hvilket element brugeren sidst har besøgt.

5 Arbejdsgange i Administrationsmodulet

5.4 Oprettelse af organisation

Forudsætninger: For at anvende Administrationsmodulet skal din organisation være oprettet i systemet. For at kunne blive oprettet som organisation, skal du enten være myndighed eller leverandør af kommunale it-systemer.

Vejledning:

1. Hvis din organisation ikke allerede er oprettet i Administrationsmodulet, skal du ansøge om at blive oprettet. Dette gør du ved at udfylde blanketten, som du finder i Tilslutningsguiden – Trin 1 i Digitaliseringskataloget.

   Bemærk: *Som ny leverandør bør du altid starte med dine opsætninger og tests i det eksterne testmiljø. Ønsker du at agere i begge miljøer (test og Produktion) skal du sætte kryds ved begge miljøer i oprettelsesblanketten.*

2. Den udfyldte og underskrevne blanket skal efterfølgende sendes til fki@kombit.dk. Bemærk at organisationen både oprettes i Administrationsmodulet og på Serviceplatformen.

3. Når forespørgslen er behandlet, får din organisation svar fra Serviceplatformens helpdesk. Svaret sendes via mail sammen med vejledning til Administrationsmodulet og NEMLOG-INs/MitID Erhvervs brugeradministration.

Resultat: Din organisation er oprettet i administrationsmodulerne **Fælleskommunalt Administrationsmodul** og i **Serviceplatformens administrationsmodul**.

5.5 Log på Administrationsmodulet

Som it-leverandør kan du have følgende roller:

Rolle	Beskrivelse
Leverandøradministrator	Giver rettigheder til at administrere it-systemer og anmode om serviceaftaler
Organisationsadministrator	Giver rettigheder til at administrere organisationens stamdata

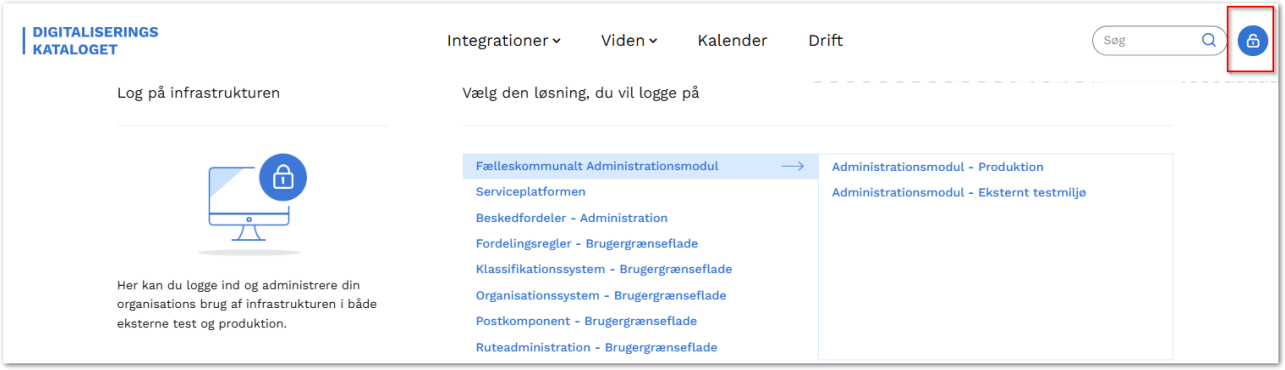
Brugeren: Med rollerne Leverandøradministrator og Organisationsadministrator kan du logge på Administrationsmodulet.

Forudsætninger: Tilknytningen af ovenstående roller sker i NEMLOG-INs administrationsmodul. Vejledningen til tilknytning af roller i NEMLOG-IN findes her.

Vejledning:

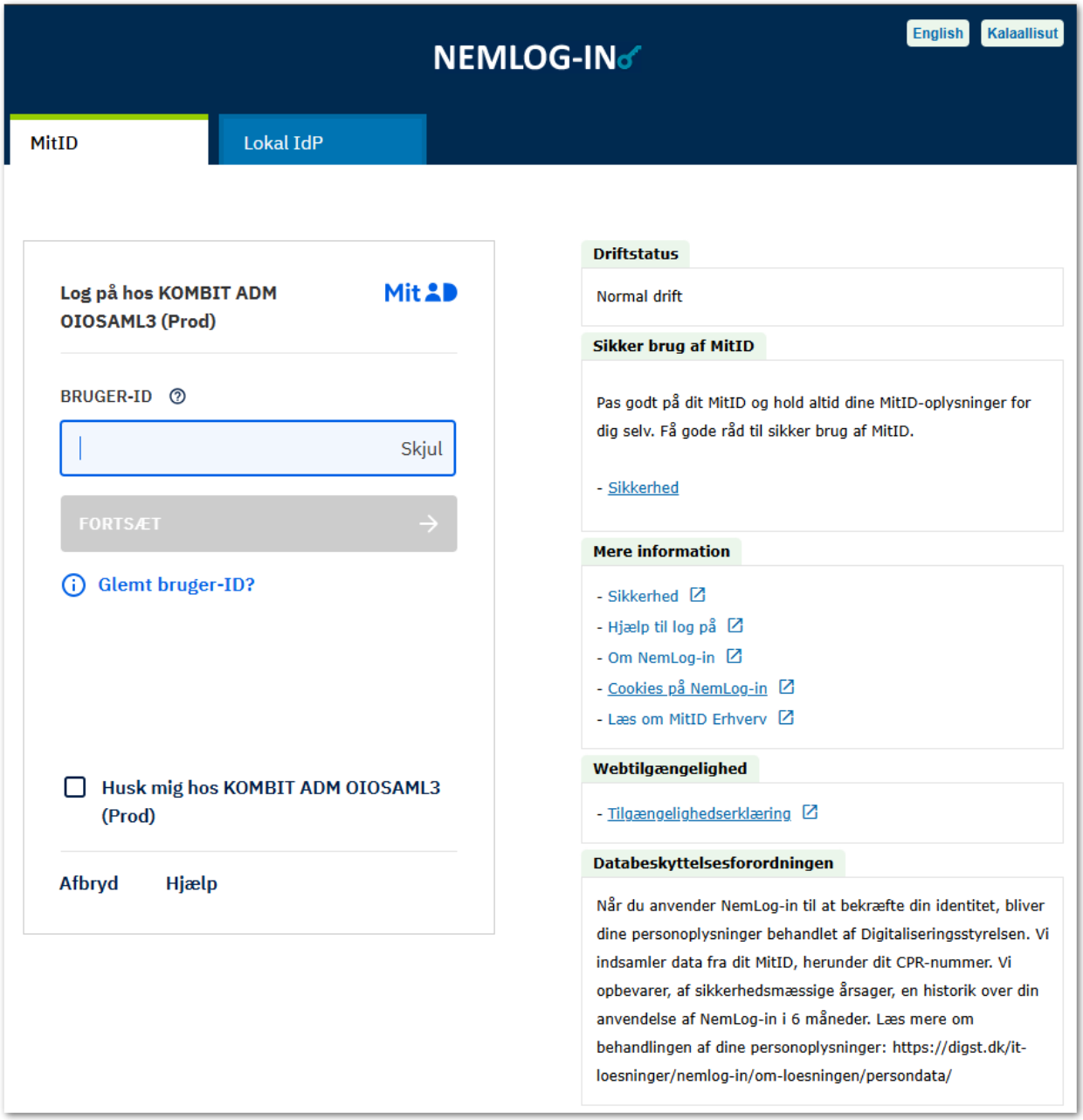
1. Du logger på Administrationsmodulet direkte via følgende links:
    - Produktionsmiljøet: admin.serviceplatformen.dk
    - Testmiljøet: admin-test.serviceplatformen.dk

2. Du kan også logge på fra Digitaliseringskataloget via log-på knappen øverst i højre hjørne.

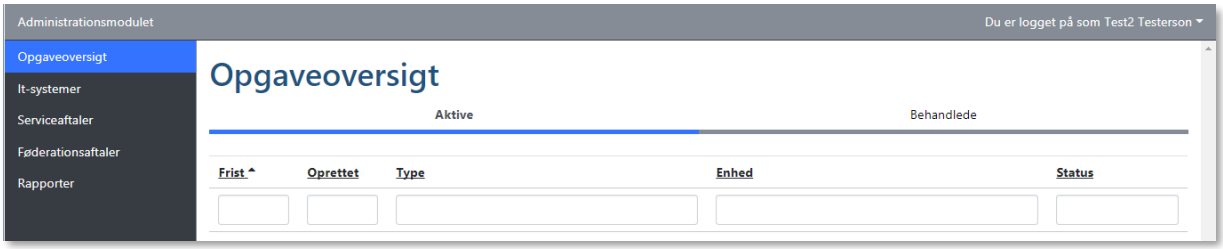


3. Du bliver herefter viderestillet til NemLog-in, hvor du skal logge på med din MitID-profil. Ved brug af MitID skal din organisations CVR-administrator på forhånd have tilknyttet din profil som medarbejder i din organisation.





4. Du er nu logget ind på Administrationsmodulet.



Resultat: Du er nu logget på Administrationsmodulet og har adgang til at se de funktioner, som din rolle berettiger dig til. Ovenfor er vist hvorledes det ser ud for rollen Leverandøradministrator.

5.6 Opgaveoversigt

Brugeren: Med rollen Leverandøradministrator og Organisationsadministrator kan du se en oversigt med opgaver, der afventer behandling, er under behandling eller er behandlet.

De opgaver der bliver vist i opgaveoversigten, afhænger af hvilken rolle din bruger har tilknyttet:

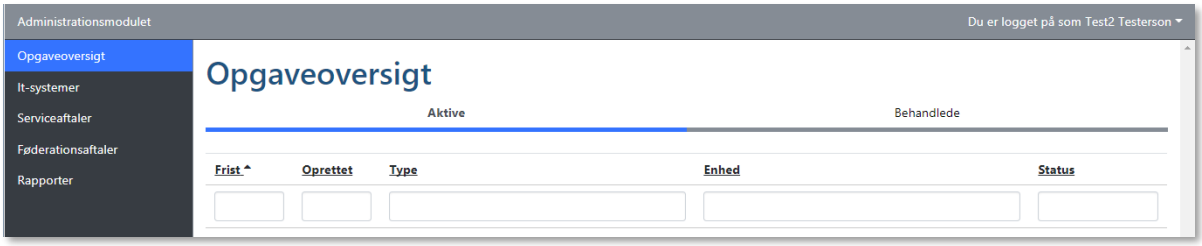
- Leverandøradministrator (bemærk at disse opgaver også kan udføres ved at gå ind på "It-systemer" i venstremenuen – se afsnit 5.8 for at se detaljer om hvordan opgaverne skal udføres)
    - Certifikatudløb – anvendersystem
    - SFTP nøgleudløb – anvendersystem
    - Certifikatudløb - callback service
    - SAML metadataudløb – brugervendtsystem
    - SAML metadataudløb – identity provider

- Organisationsadministrator (bemærk at denne opgave også kan udføres ved at gå ind på "Organisationer" i venstremenuen – se afsnit 5.21 for at se detaljer om hvordan opgaven skal udføres)
    - Certifikatudløb - organisation

Vejledning:

1. I Administrationsmodulet skal du vælge punktet Opgaveoversigt i venstremenuen. Herefter får du et overblik over organisationens opgaver, som kan have status "Afventer behandling", "Under behandling" eller "Behandlet".
   Du kan fremsøge en opgave ved at søge i felterne Frist, Oprettet, Type, Enhed og Status. Vælg en opgave fra listen ved at klikke på den.

   For at få overblik over opgaver der afventer behandling vises de under fanen "Aktive" eller de opgaver der er behandlet findes under fanen "Behandlede". Begge faner fremgår af skærmbilledet nedenfor.

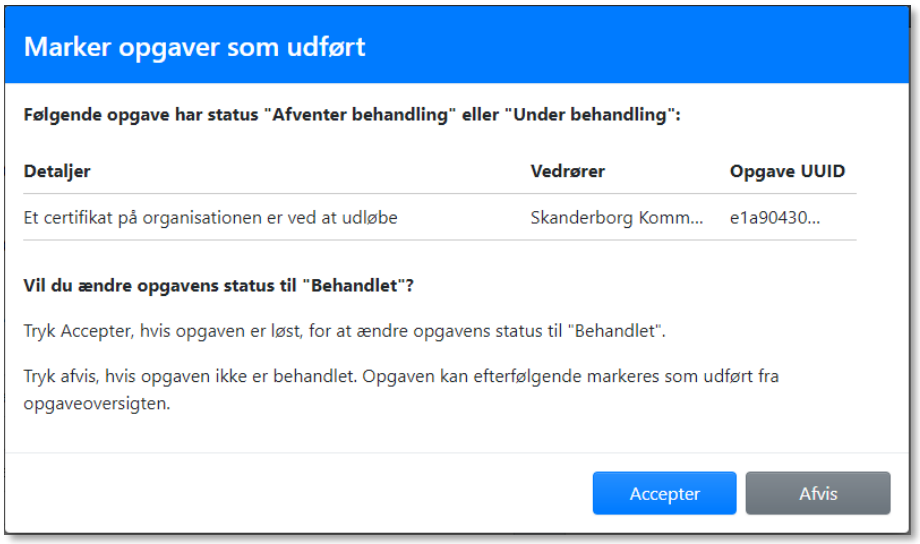


2. Når du vælger en opgave fra listen som afventer behandling, kan du se opgaven og vælge at gå i gang med opgaven ved at trykke på "Start behandling". Herefter vil status for opgaven ændre sig til "Under behandling". Hvis du blot ønsker at se systemet eller aftalen som opgaven er relateret til, kan du trykke på knappen "Vis", så ændrer status på opgaven sig ikke.

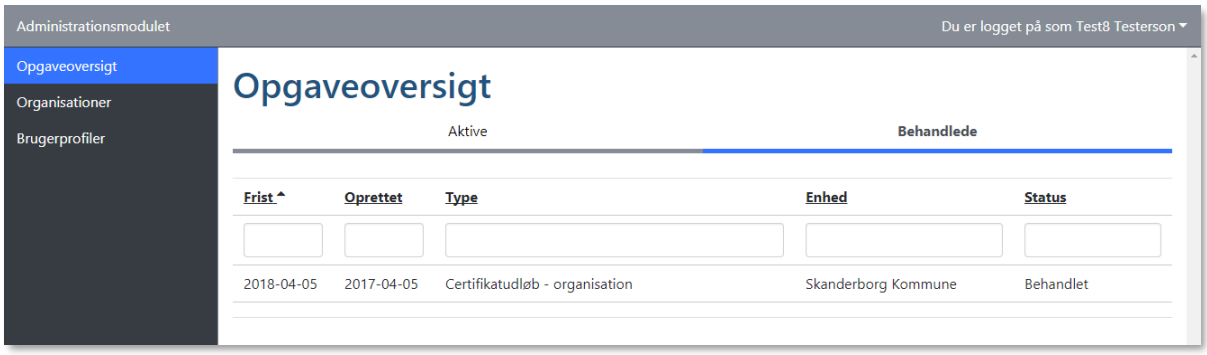


3. Efter du har trykket på knappen ”Start behandling” for en opgave, bliver du ført videre til der, hvor du skal udføre opgaven.

4. Når du har udført opgaven, vises en dialog med opgaven og andre relaterede opgaver, der ikke er markeret som udført. Relaterede opgaver er opgaver på samme organisation eller it-system. Du kan her vælge at markere opgaverne som udført ved at trykke på knappen ”Accepter” eller afvise ved at trykke på knappen ”Afvis”.



5. Når du har trykket på ”Accepter” eller ”Afvis” kommer du tilbage til opgaveoversigten. Hvis du har accepteret, vil alle opgaver i dialogen automatisk være flyttet til oversigten over behandlede opgaver, som findes under fanen ”Behandlede”, som nedenfor er markeret med blåt.



Hvis du har afvist, vil ingen af opgaverne i dialogen ændre status. Opgaverne kan derfor stadig findes i oversigten over aktive opgaver. Vælger du opgaven igen, kan du markere den som udført ved at trykke på knappen ”Marker som udført”.



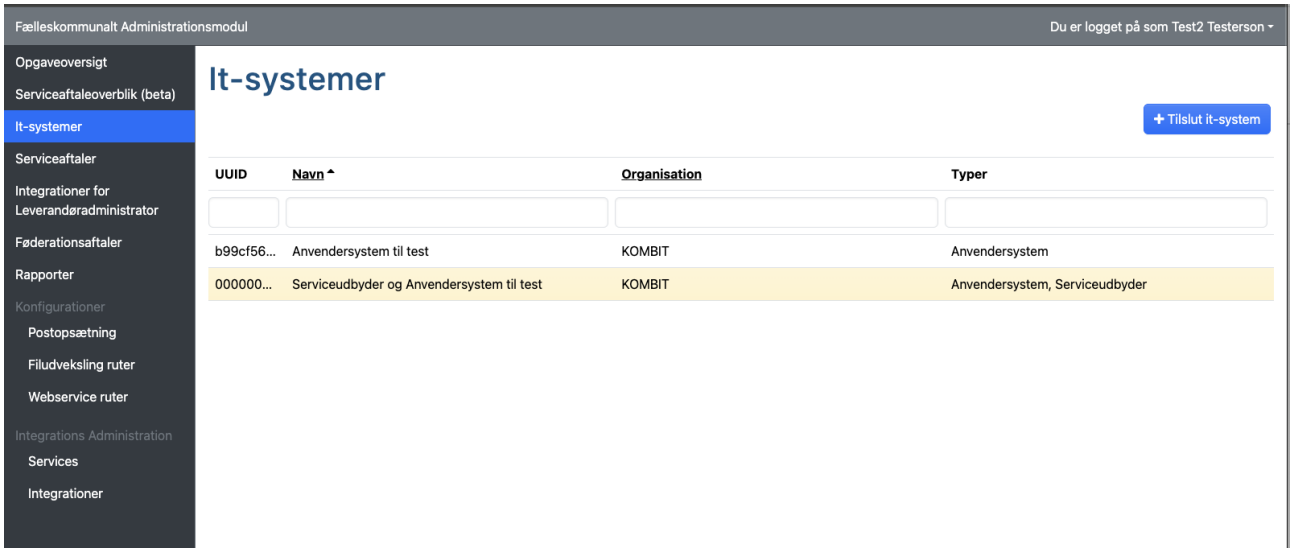
Resultat: Du har fået overblik over din organisations opgaver, og har evt. ændret status på en opgave fra ”Afventer behandling” til ”Under behandling” eller til ”Behandlet”.

5.7 Tilslut it-system

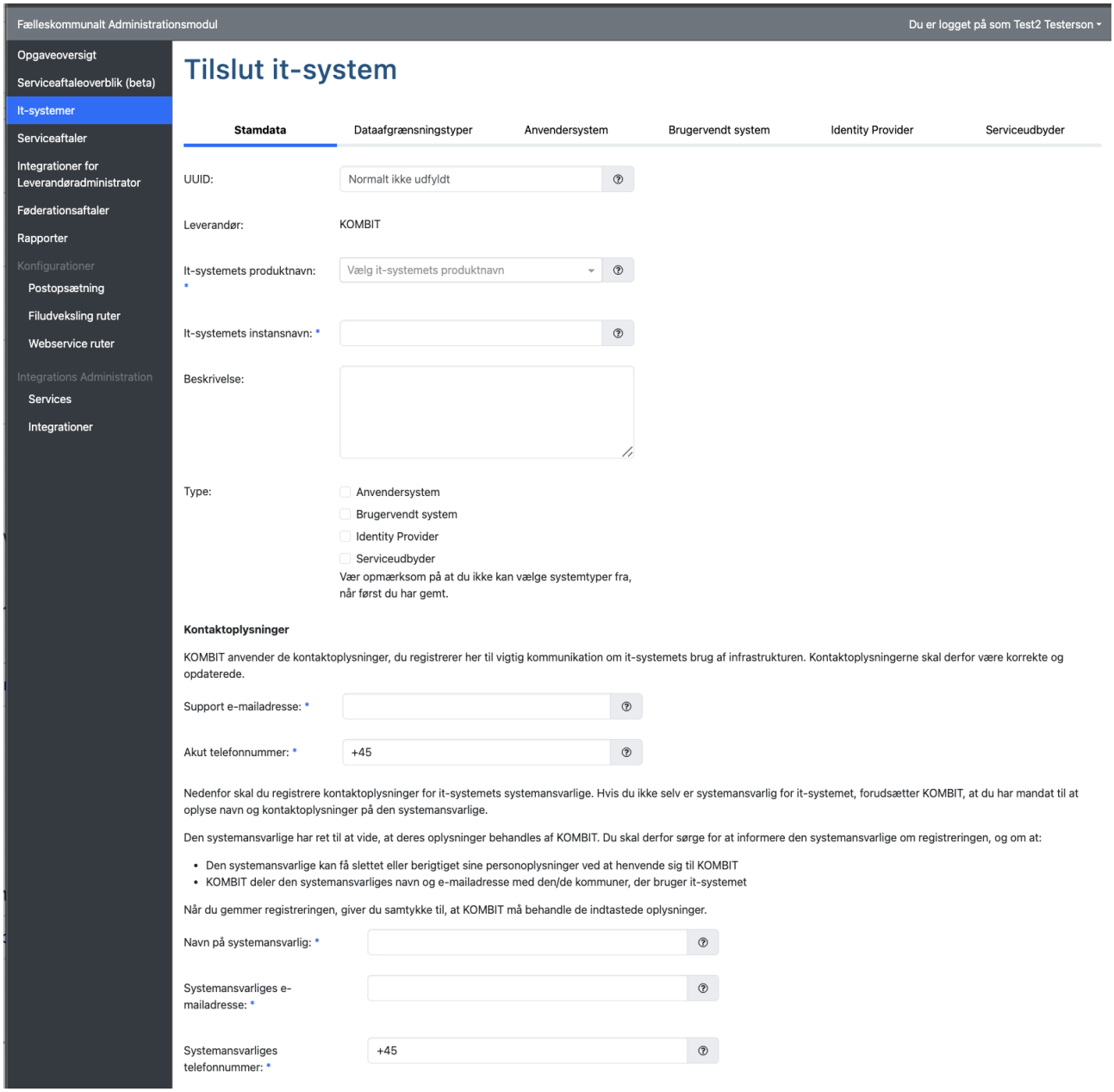
Brugeren: Med rollen Leverandøradministrator kan du tilslutte et it-system.

Vejledning:

I Administrationsmodulet skal du vælge punktet It-systemer i venstremenuen. For at tilslutte et nyt it-system skal du trykke på knappen ”Tilslut it-system”.



5.7.1 Stamdata



Udfyld følgende oplysninger på fanen Stamdata:

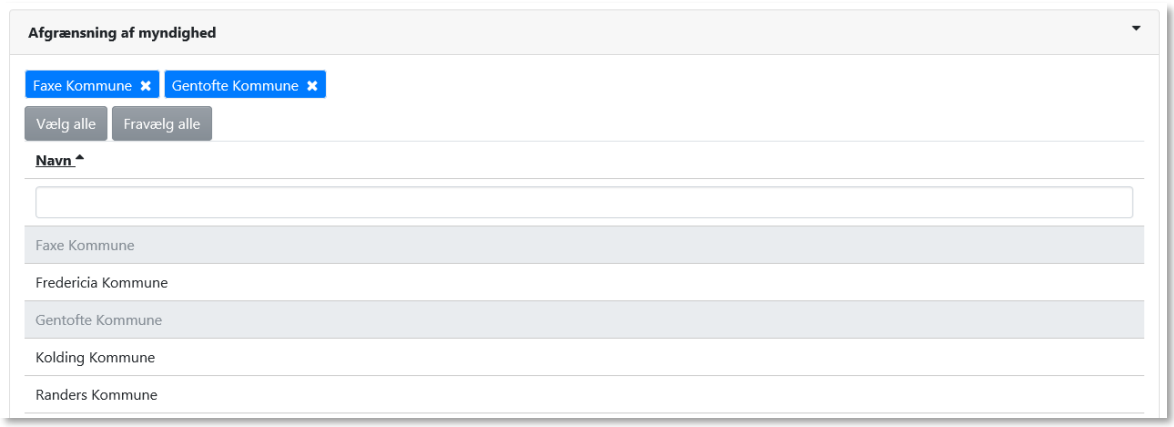
- UUID: Dette felt udfyldes normal ikke, men har du behov for at dit system får et bestemt UUID, f.eks. hvis du vil have samme UUID på tværs af miljøer eller du på anden vis er afhængig af en bestemt UUID, kan du her indtaste den unikke nøgle for it-systemet. Hvis feltet ikke udfyldes, autogeneres et UUID når du gemmer (bemærk at du ikke efterfølgende kan ændre UUID).
- It-systemets produktnavn: Her skal du vælge det produktnavn, som it-systemet kendes under. Listen af valgmuligheder er defineret af KOMBIT for hver enkelt leverandør. Hvis ikke der findes et relevant produkt i listen skal der vælges 'System mangler'
- It-systemets instansnavn: Skriv et sigende navn på det it-system, du ønsker at tilslutte.
- Beskrivelse: Tilføj en beskrivelse af it-systemet (er valgfrit at udfylde).

- Type: Vælg én eller flere af følgende systemtyper
    - Anvendersystem: Et it-system der anvender en service, hvor aftaler om adgang til servicen styres via serviceaftaler.
    - Brugervendt system: Et it-system der udstiller sikret og adgangsbeskyttet brugergrænseflade, der tilgås via en browser.
    - Identity Provider: Et it-system der udsteder tokens med rettigheder for en (eller flere) myndighed(ers) brugere.
    - Serviceudbyder: Et it-system der tilbyder service. En service tilbudt af en serviceudbyder tilgås ofte af et Anvendersystem via en tilkoblet service på Serviceplatformen.

  Afhængig af hvilke type der vælges, aktiveres de tilhørende faner, hvor der oprettes data tilknyttet den specifikke systemtype. Se uddybende beskrivelse af fanerne i de følgende afsnit. Vær opmærksom på at når først du har gemt it-systemet, så kan du ikke fravælge allerede valgte typer, du kan dog tilføje en ny type.
- Kontaktoplysninger: Disse anvendes af KOMBIT til vigtig kommunikation om it-systemets brug af infrastrukturen. Kontaktoplysningerne skal derfor være korrekte og opdaterede. De omfatter:
    - Support e-mailadresse: Denne postkasse skal ikke være personlig, da personlige postkasser er for sårbare i forhold til personaleskift. KOMBIT sender vigtige meddelelser til denne postkasse: Fx varsler om udfasninger og anmodninger om opdatering af kontaktoplysninger.
    - Akut telefonnummer: Akut telefonnummeret må ikke være personligt, da det anvendes til akut kontakt ved fx fejl. Det er derfor vigtigt, at KOMBIT kan komme i kontakt med supporten for it-systemet i et så stort et tidsrum som muligt.
    - Navn på systemansvarlig: Navn på den person i organisationen, der er ansvarlig for systemet. KOMBIT kontakter den systemansvarlige, hvis der er behov for dialog. Navnet bliver vist for de kommuner, som anvender it-systeminstansen.
    - Systemansvarliges e-mailadresse: Som udgangspunkt er denne e-mailadresse personlig. KOMBIT kontakter den systemansvarlige, hvis der er behov for dialog. E-mailadressen bliver vist for de kommuner, som anvender systeminstansen.
    - Systemansvarliges telefonnummer: Som udgangspunkt er dette telefonnummer personligt. KOMBIT kontakter den systemansvarlige, hvis der er behov for dialog.

- Afgrænsning af myndighed: Afgrænsning af myndigheder også kaldet en ”whitelist” betyder, at det kun er de myndigheder, man vælger på listen som har tilladelse til at bruge it-systemet. Omvendt betyder det, at hvis ikke man har valgt nogle myndigheder på listen ”Afgrænsning af myndighed”, betyder det, at alle myndigheder må bruge it-systemet.

  Hvis du ønsker at afgrænse hvilke myndigheder, der må have tilladelse til at tilgå it-systemet, skal du vælge den eller de relevante myndigheder fra listen, som vist nedenfor. Du kan fremsøge en myndighed via feltet Navn. Vælg myndigheden ved at klikke på den fra listen.

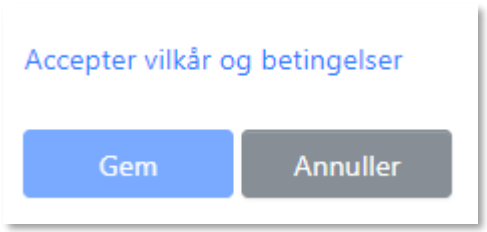


De afgrænsninger af myndigheder, du vælger for it-systemet, bliver anvendt på:

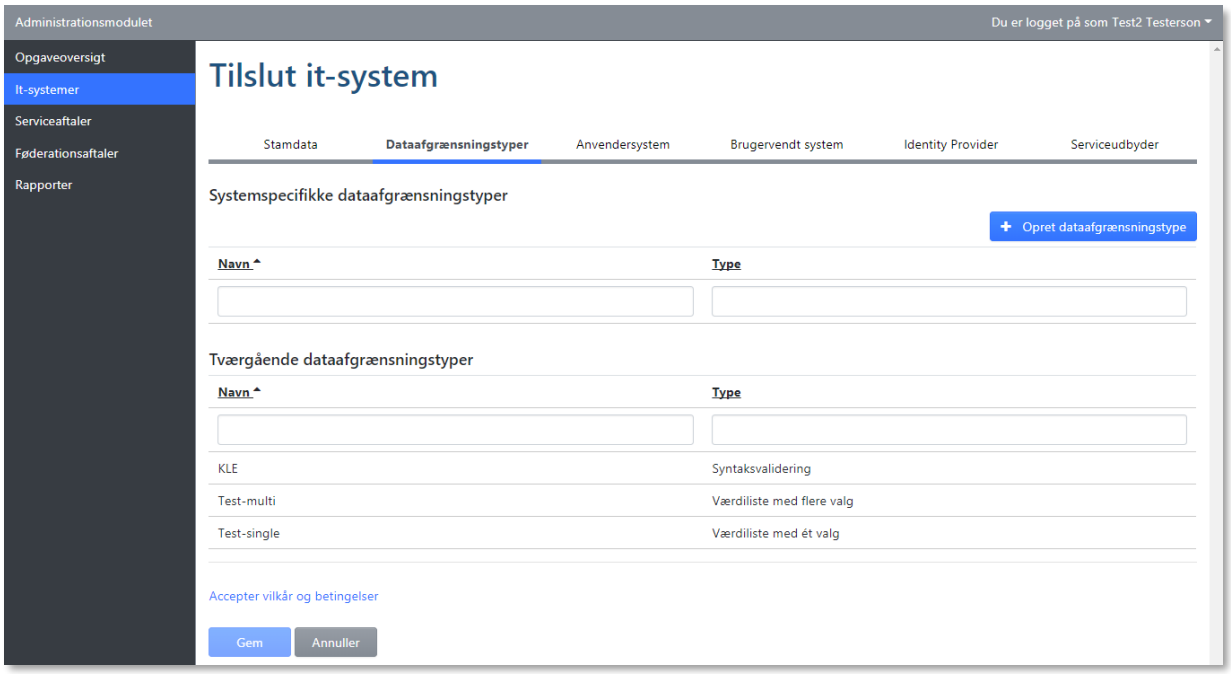
- Serviceaftaler
- Føderationsaftaler
- Jobfunktionsroller

Gem it-system

Bemærk: Det er muligt at gemme undervejs. Før du kan gemme et it-system, skal du klikke på linket "Accepter vilkår og betingelser" som vises i bunden af hver fane. Når du har accepteret vilkår og betingelserne, skal du efterfølgende trykke "Gem", hvorefter du kommer tilbage til oversigten over it-systemer.



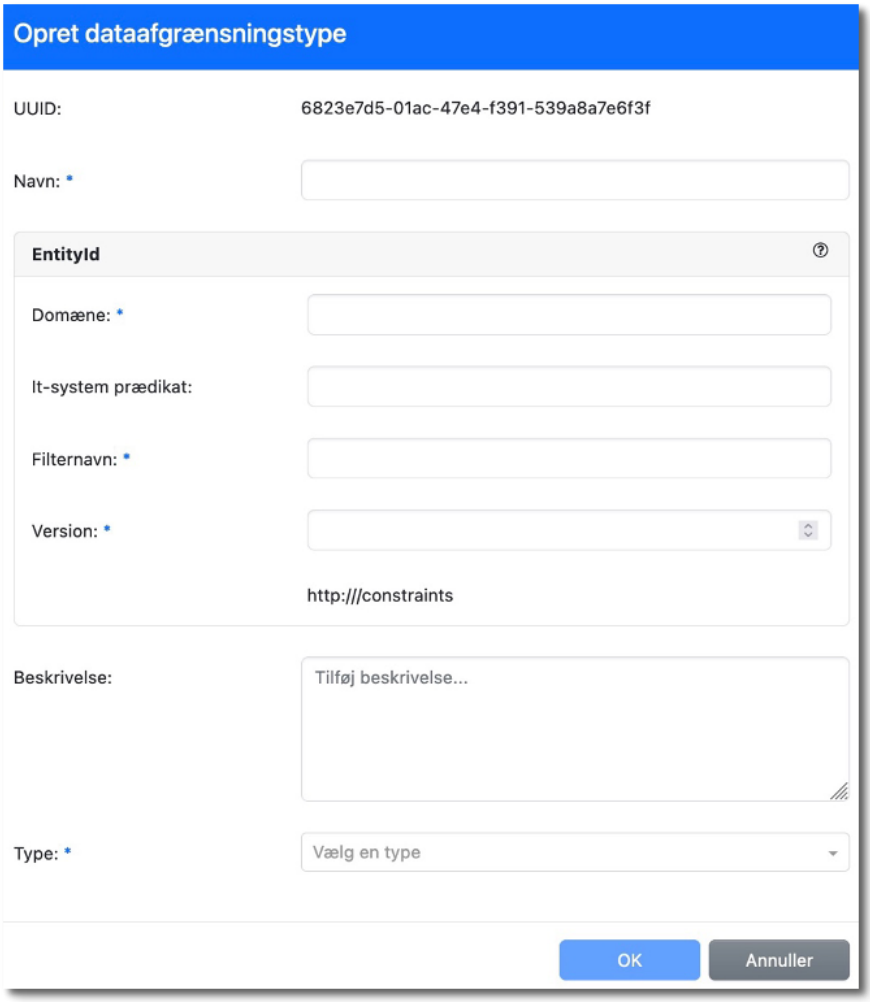
5.7.2 Dataafgrænsningstyper



Hvis du har valgt en systemtype der anvender dataafgrænsninger (Brugervendt system, eller Serviceudbyder), kan du på denne fane tilknytte dataafgrænsningstyper til systemet. Dataafgrænsninger er fælles for brugervendt system og serviceudbyder. Du kan oprette systemspecifikke dataafgrænsninger og få vist de tværgående dataafgrænsningstyper, der allerede findes. De tværgående dataafgrænsninger er på forhånd defineret af KOMBIT, og kan derfor ikke ændres. Du kan klikke på dataafgrænsningstypen og få vist, hvilke oplysninger dataafgrænsningstypen indeholder.

Bemærk: Dækker en af de tværgående dataafgrænsningstyper dit behov, skal denne bruges, og der skal ikke oprettes en ny systemspecifik dataafgrænsningstype. Grunden hertil er, at de tværgående dataafgrænsningstyper indeholder pre-definerede værdilister eller syntaksvalidering.

For at oprette en ny systemspecifik dataafgrænsning skal du trykke på knappen ”Opret dataafgrænsningstype”.



Udfyld følgende oplysninger for at oprette systemspecifikke dataafgrænsningstyper:

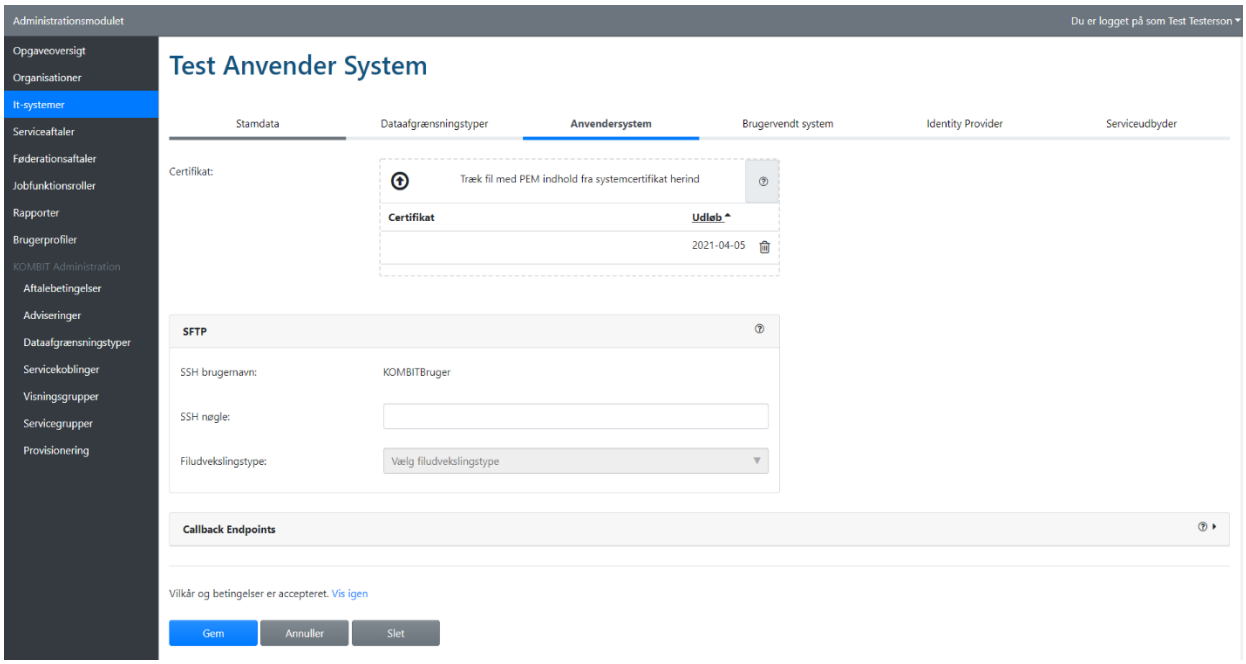
- Navn: Giv dataafgrænsningstypen et sigende navn
- EntityId: Udfyld med oplysninger om Domæne, It-system prædikat,Filternavn og Version. Det unikke navn for dataafgrænsningstypen, som skal skrives på formen http://<Domæne>/constraints/<It-system prædikat>/<Filternavn>/<Version>. Det kunne eksempelvis være http://entityid.kombit.dk/constraints/bfo/beskedtype/1, hvor 'bfo' angiver Beskedfordeler.
    - <domæne> skal bestå af mindst to led adskilt med punktum, hvert led skal bestå af mindst to tegn, hvor tilladte tegn er a-z, A-Z, 0-9 samt bindestreg og underscore, dog må første tegn i et led ikke være bindestreg eller underscore.
    - <It-system prædikat> er valgfrit, og kan indeholde en forkortelse, kaldenavn eller lignede for det system, dataafgrænsningen er oprettet til. Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <It-system prædikat> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
    - <filternavn> Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <filter> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
    - <version> skal være et heltal mellem 1 og 99.

- Beskrivelse: Tilføj en beskrivelse, fx hvilke værdier, der er tilladte (er valgfrit at udfylde, men er kritisk for, at brugeren kan beslutte hvilken værdi, der skal anvendes i anmodning af en serviceaftale)
- Type: Vælg en type fra listen (bemærk at de dataafgrænsningstyper og mulige værdier der tilføjes, skal svare til de dataafgrænsningstyper og værdier som systemet kan håndhæve):
    - Ved typen Syntaksvalidering, kommer der et felt, hvor du skal indtaste et regulært udtryk.
    - Ved typen Værdiliste med ét valg, kommer der en liste, hvor du kan tilføje værdier ved at trykke på knappen "Tilføj værdi".
    - Ved typen Værdiliste med flere valg, kommer der en liste, hvor du kan tilføje værdier ved at trykke på knappen "Tilføj værdi".

      Bemærk de to værdilister ser ens ud i oprettelsen, der er først forskel, når du skal bruge dem i praksis, hvor man så enten kan vælge én værdi eller flere værdier.

Afslut med at trykke "Ok", hvorefter du kommer tilbage til fanen Dataafgrænsningstyper.

5.7.3 Anvendersystem



Udfyld følgende oplysninger på fanen Anvendersystem:

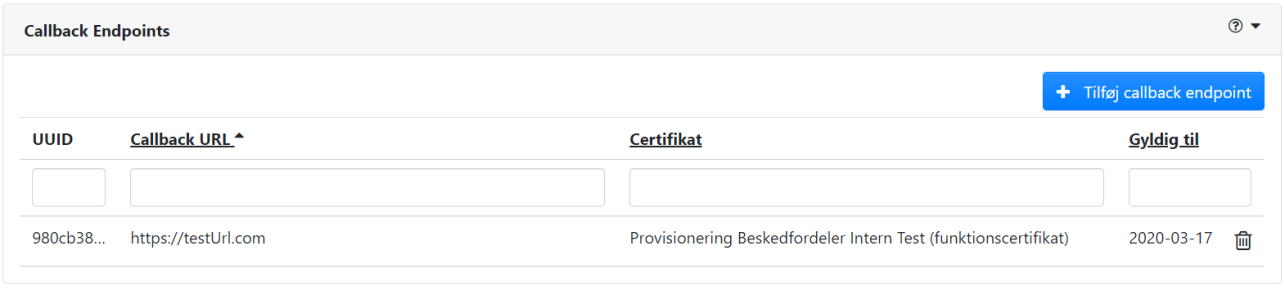
- Certifikat: Tilføj systemcertifikatet ved at trække certifikatet ind på det markerede område. Der gælder følgende regler for certifikater:
    - Skal være unikt og må ikke genanvendes på andre systemer
    - Systemet må gerne have flere gyldige certifikater
    - Skal være et Organisations- eller Systemcertifikat.
    - Certifikatet skal være et base64 encoded X509-certifikat.

- SFTP: Udfyldes kun hvis du benytter SFTP. Her skal du indtaste SSH brugernavn, SSH-nøgle og vælge Filudvekslingstype. Disse parametre skal udfyldes på følgende måde:
    - Brugernavn: Det brugernavn som benyttes som identifikation, når andre it-systemer ønsker at sende filer til dit it-system. Samtidig anvendes brugernavnet til at logge ind på SFTP

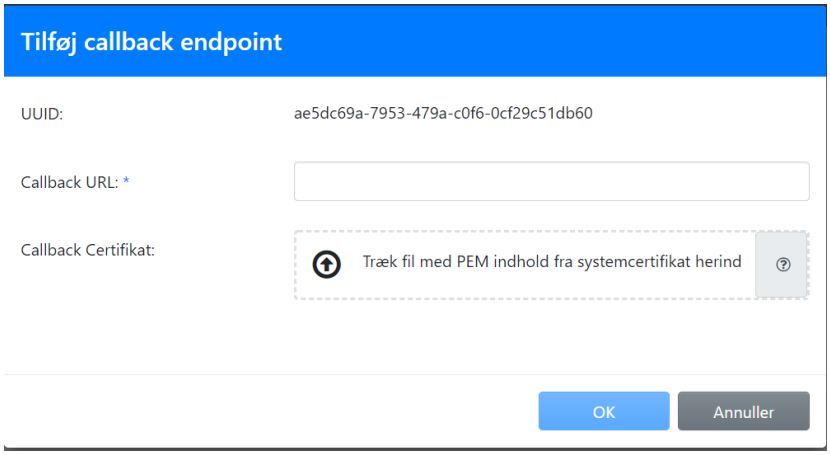
serveren. Brugernavnet kan ikke ændres efter at it-systemet er blevet oprettet, hvorfor det er vigtigt, at du vælger det med omhu.
    - Bemærk, at systemet tilbyder mulighed for at generere et SFTP-brugernavn ved klik på "Klik her for at lade systemet foreslå et unikt brugernavn". Det foreslåede brugernavn kan evt. redigeres, før systemet gemmes.
- Offentlig SSH-nøgle: Et it-system logger på SFTP-serveren ved brug af SSH-nøgler. For at Serviceplatformen (som denne information provisioneres til) kan give et it-system adgang til SFTP serveren, skal Serviceplatformen kende den offentlige del af den SSH-nøgle, som it-systemet vil bruge til at logge på SFTP serveren med. Det er muligt at genbruge samme SSH-nøgle til flere af din organisations it-systemer. Du kan finde en vejledning til generering af en SSH-nøgle i afsnit i dokumentet SP-G2 USM0005 Vejledning til Serviceplatformens SFTP Service Vejledning til Serviceplatformens SFTP Service.
    - Bemærk, at systemet tilbyder mulighed for at generere et nyt SFTP-nøglepar ved klik på "Klik her for at lade systemet generere et nøglepar". Ved anvendelse af denne mulighed bliver den offentlige nøgle automatisk gemt sammen med systemets øvrige data, mens den private nøgle skal kopieres og installeres i Anvendersystemets afviklingsplatform. Den private nøgle gemmes ikke i systemet, hverken i Administrationsmodulet eller i Serviceplatformen.
- Vælg hvilken filudvekslingstype it-systemet vil anvende SFTP servicen med. Bemærk, at der fremadrettet kun er mulighed for at vælge typen "Simpel".
- Læs og godkend vilkårene for oprettelse af et it-system med SFTP tilvalgt.

  Bemærk, at Administrationsmodulet og Serviceplatformen fremadrettet håndhæver, at SFTP-nøgler skal udskiftes hvert andet år. Når en nøgle er udløbet, kan der ikke længere opnås adgang til SFTP-kontoen med denne nøgle. Filer, der ligger på SFTP-kontoen, bliver ikke slettet, og rutninger til SFTP-kontoen vil også fortsat fungere, men der skal knyttes en ny nøgle til kontoen, før der igen kan opnås adgang til disse filer.

- Callback Endpoints: Der skal eksistere callback endpoints hvis man ønsker at systemet skal kunne indgå i serviceaftaler hvor der vælges callback services.

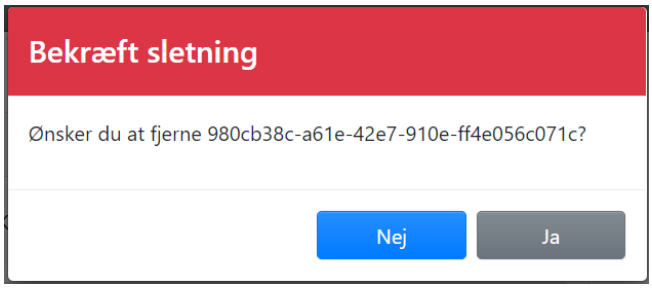


    - Tilføj callback endpoint/Redigér callback endpoints: gøres ved tryk på den blå tilføj knap eller ved tryk på det pågældende callback endpoint.



- UUID: Uuid for callback endpointet, sættes automatisk.
- CallbackURL er krævet og skal være en valid Https URL.
- CallbackCertifikat er krævet og skal være et base64 encoded X509-certifikat. Det må gerne genanvendes på andre callback endpoints såfremt disse endpoints ikke har ens URL.

- Fjern callback endpoint: gøres ved at man trykker på skraldespands-ikonet ud fra pågældende callback endpoint.



5.7.4 Brugervendt system

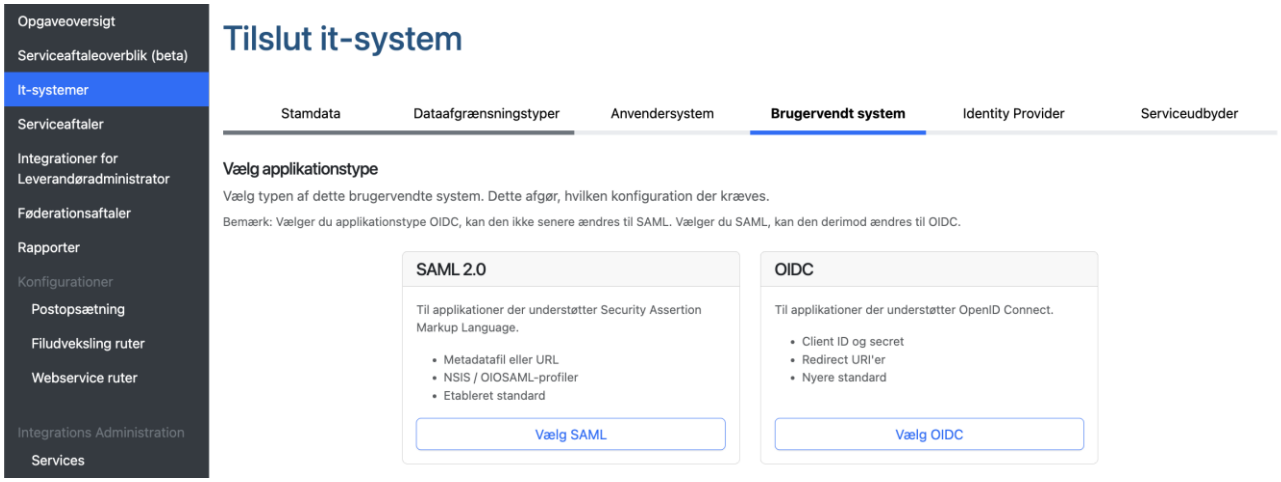
Et brugervendt system tilmeldt den fælleskommunale infrastruktur skal understøtte en af følgende to standarder for bruger login/logout: Security Assertion Markup Language (SAML) eller OpenID Connect (OIDC).

Ved oprettelse af et brugervendt system skal det oplyses, om systemet har applikationstypen SAML eller OIDC. Dette valg indikerer, hvilken af de to standarder, der understøttes.

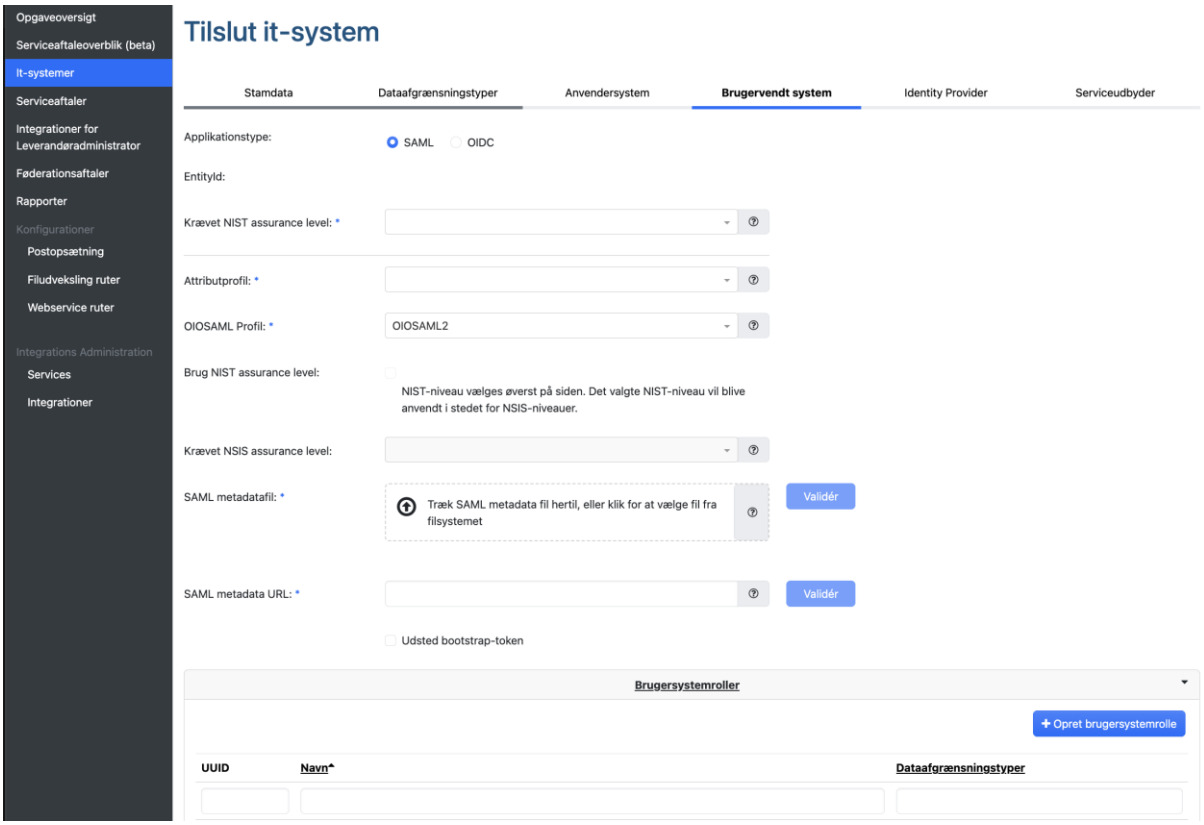
I den fælleskomunale infrastruktur er understøttelse for OIDC-standarden blevet indført senere end for SAML-standarden. Systemer, der er oprettet, før OIDC-standarden blev indført, har applikationstypen SAML.

Når et system er blevet gemt, er det muligt efterfølgende at skifte applikationstypen fra SAML til OIDC (mere herom nedenfor) men ikke den modsatte vej.

Valget af applikationstype har betydning for, hvilke oplysninger, der skal indtastes for systemet.



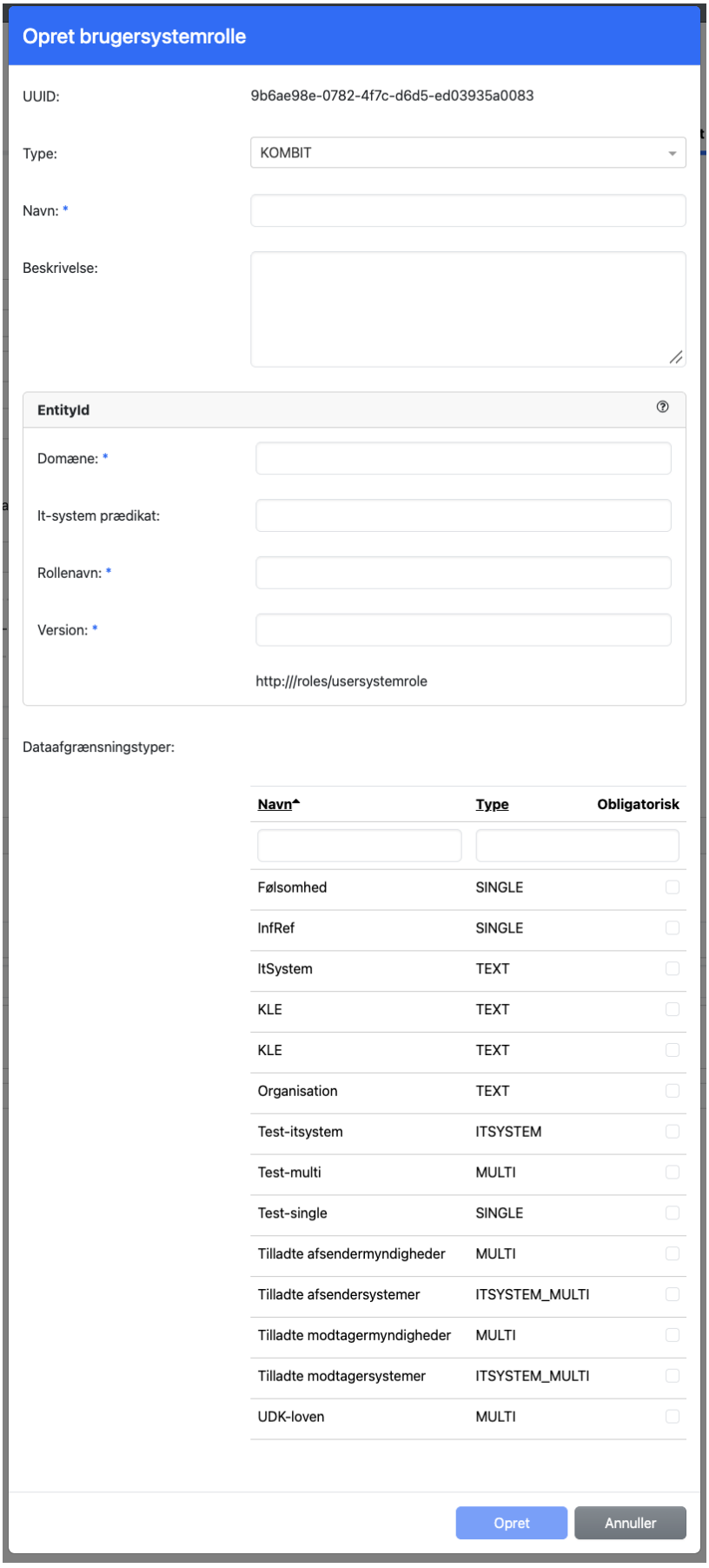
Oplysninger for et brugervendt system, der understøtter SAML:



Udfyld følgende oplysninger på fanen Brugervendt system (SAML-variant):

- Krævet NIST assurance level:
  Du har fire forskellige sikkerhedsniveauer at vælge imellem:
  - Niveau 1 – Lille eller ingen tiltro til påstået identitet
  - Niveau 2 – Nogen tiltro til påstået identitet
  - Niveau 3 – Høj tillid til påstået identitet

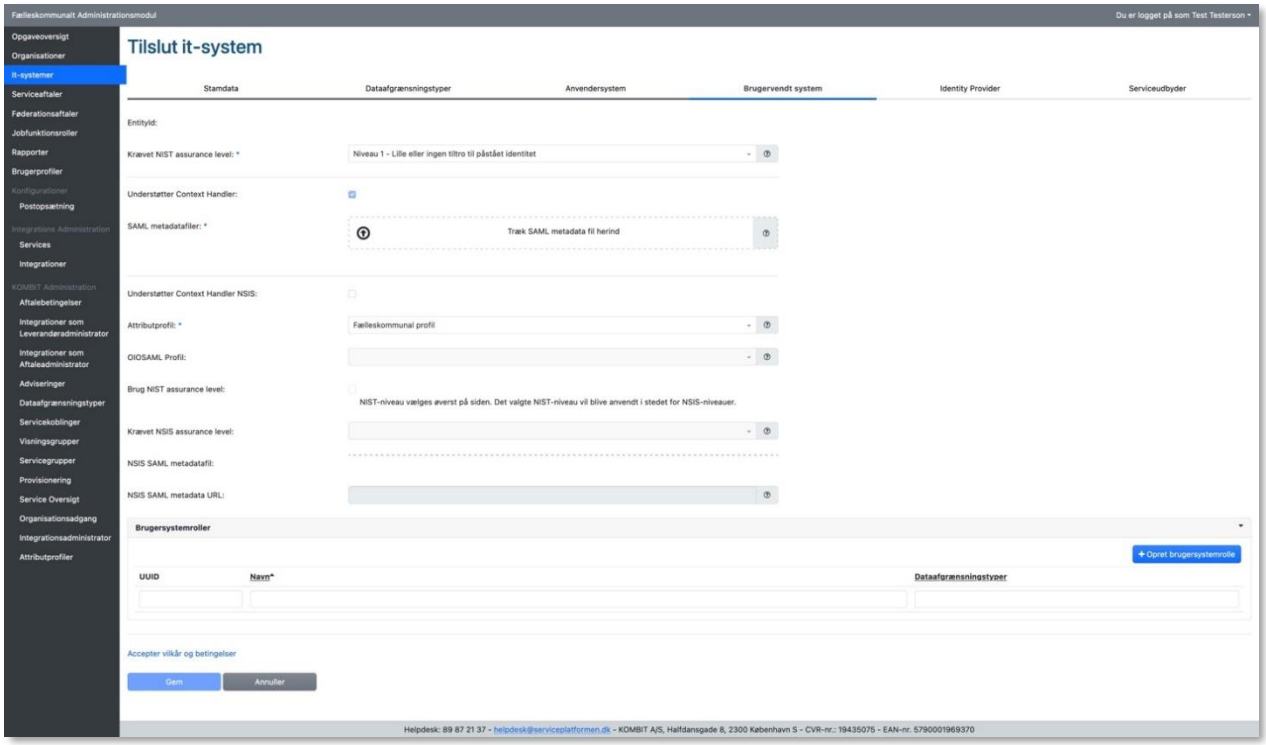
    - Niveau 4 – Meget høj tillid til påstået identitet
- Attributprofil: Valget af attributprofil afgør, hvilke brugeroplysninger der udstilles i tokens. Som standard vil et brugervendt system benytte attributprofilen "Fælleskommunal profil". Alternativt kan vælges "Fælleskommunal profil uden persondata" eller ”SEB Profil”.
- OIOSAML Profil: Det er ikke muligt at oprette egne OIOSAML profiler, men der er to valgmuligheder til rådighed: *OIOSAML2* og *OIOSAML3*. Bemærk at NSIS assurance level er inaktiv, hvis *OIOSAML3* profilen anvendes.
- Brug NIST assurance level: Kan kun vælges, hvis der samtidig benyttes OIOSAML3 profil. I så fald vil NIST assurance level som anført under ”Krævet NIST assurance level” blive benyttet sammen med OIOSAML3-profilen (som en undtagelse tilladt af Digitaliseringsstyrelsen). Hvis fravalgt samt der bruges OIOSAML3 profil, bliver NSIS assurance level som anført under ”Krævet NSIS assurance level” brugt.
- Krævet NSIS assurance level. For at sikre en hensigtsmæssig sikkerhed i NSIS, kræves et specifikt sikkerhedsniveau. Bemærk venligst, at hvis et sådant niveau er påkrævet, skal alle kommunale brugere være i stand til at levere dette niveau. Det er ikke muligt at skræddersy sikkerhedsniveauer i NSIS, så du har valget imellem tre prædefinerede valgmuligheder:
    - Lav
    - Betydelig
    - Høj.
- SAML metadatafil: SAML metadatafilen indeholder blandt andet bindings og location for SAML services og it-systemets offentlige nøgle baseret på et Organisations- eller Systemcertifikat. Træk din SAML metadatafil ind på det markerede område. Alternativt kan der angives en SAML metadata URL.
    - SAML metadatafilen bliver valideret af Context Handler, inden den kan gemmes og benyttes. Hvis metadatafilen indeholder fejl, kan systemet ikke gemmes. Det anbefales, at du efter upload aktiverer knappen ’Validér’. Herved sendes filen til validering hos Context Handler, og eventuelle fejl (blokerende for gemning) og advarsler (ikke-blokerende) vil blive vist, så du har mulighed for at tilrette og uploade på ny.
- SAML metadata URL: I stedet for at uploade en SAML metadatafil, kan man angive en URL hvor metadata kan hentes fra. URL’en skal være valid, og skal derudover være med https protokol. Der er samme krav til indholdet af metadata, som hvis den blev uploadet direkte på Administrationsmodulet.
    - SAML metadata-URL’en bliver valideret af Context Handler, inden den kan gemmes og benyttes. Context Handler hjemhenter metadatafilen ved at kalde metadata-URL’en, og hvis URL’en er utilgængelig eller den hjemhentede metadatafil indeholder fejl, kan systemet ikke gemmes. Det anbefales, at du efter indtastning af URL’en aktiverer knappen ’Validér’. Herved sendes URL’en til validering hos Context Handler, og eventuelle fejl (blokerende for gemning) og advarsler (ikke-blokerende) vil blive vist, så du har mulighed for at rette manglerne. Dette kan indebære tilpasninger til den service, som metadata-URL’en henviser til.
- Udsted bootstrap-token: Hvis dette felt er markeret, udsteder Context Handler Bootstrap tokens for dette brugervendte system.
- Brugersystemrolle: For at oprette en brugersystemrolle tryk på ”Opret brugersystemrolle”. Bemærk at de brugersystemroller der oprettes, skal svare til de brugersystemroller som systemet kan håndhæve.

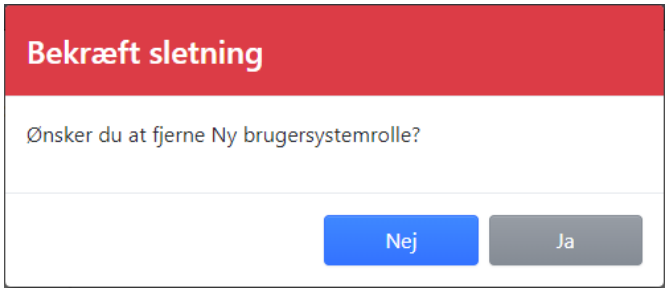

Opret brugersystemrolle
UUID:
9b6ae98e-0782-4f7c-d6d5-ed03935a0083
Type:
KOMBIT
Navn: *
Beskrivelse:
EntityId
Domæne: *
It-system prædikat:
Rollenavn: *
Version: *
http:///roles/usersystemrole
Dataafgrænsningstyper:
Navn
Type
Obligatorisk
Følsomhed SINGLE
InfRef SINGLE
ItSystem TEXT
KLE TEXT
KLE TEXT
Organisation TEXT
Test-itsystem ITSYSTEM
Test-multi MULTI
Test-single SINGLE
Tilladte afsendermyndigheder MULTI
Tilladte afsendersystemer ITSYSTEM_MULTI
Tilladte modtagermyndigheder MULTI
Tilladte modtagersystemer ITSYSTEM_MULTI
UDK-loven MULTI
Opret
Annuller

Udfyld følgende oplysninger for at oprette en brugersystemrolle:

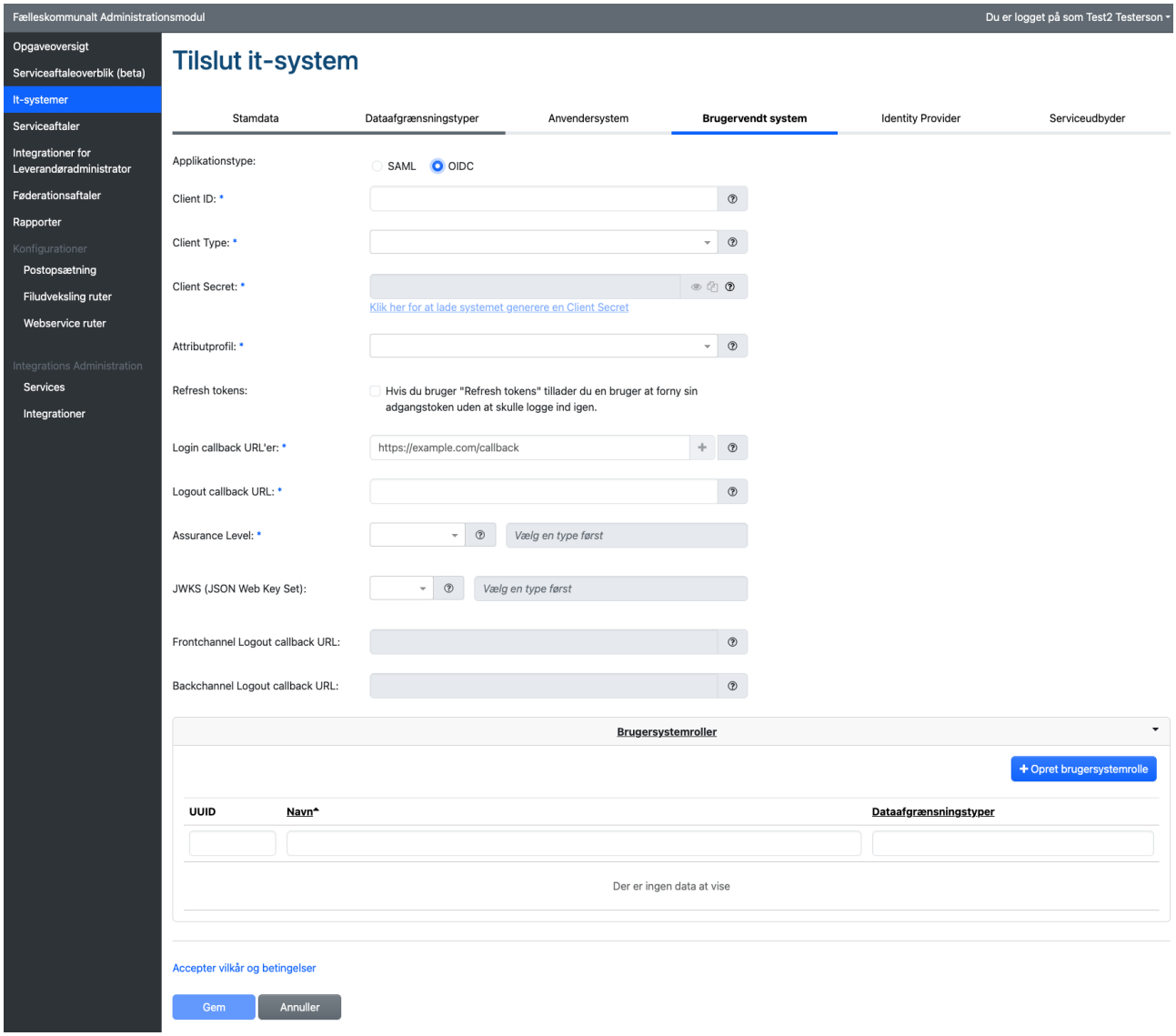
- Type: Vælg en type blandt mulighederne KOMBIT, SEB og NSP
  - Typen KOMBIT er forvalgt.
  - Alle brugersystemroller, som er blevet oprettet i systemet, før det blev muligt at vælge type, er af typen KOMBIT.
  - Typen SEB kan kun vælges for brugervendte systemer med attributprofilen "SEB-profil". Hvis denne regel ikke er opfyldt, kan det brugervendte system ikke gemmes.
  - Resten af siden tilpasser sig valget af type:
    - Strukturen af EntityId er unik for hver type
    - NSP-typen tillader ikke brug af dataafgrænsningstyper men giver til gengæld mulighed for indlejring i bootstrap-token
  - Type kan ikke ændres for en allerede gemt rolle.
- Indlejret i bootstrap-token: Hvis markeret, indlejres rollen i bootstrap-token. Denne mulighed gives kun for NSP-typen.
- Navn: Giv brugersystemrollen et sigende navn
- Beskrivelse: Tilføj en beskrivelse (er valgfrit at udfylde).
- EntityId for typen KOMBIT: Udfyld med oplysninger om Domæne, It-system prædikat (Valgfrit), Filternavn og Version. Det unikke entityId for brugersystemrollen skabes ud fra disse oplysninger og får følgende form: http://<Domæne>/roles/usersystemrole/<It-system prædikat>/<Rollenavn>/<Version>. Det kunne eksempelvis være http://sts.kombit.dk/usersystemrole/BFO/Testrolle/1, hvor BFO angiver Beskedfordeler.
  - <domæne> skal bestå af mindst to led adskilt med punktum, hvert led skal bestå af mindst to tegn, hvor tilladte tegn er a-z, A-Z, 0-9 samt bindestreg og underscore, dog må første tegn i et led ikke være bindestreg eller underscore.
  - <It-system prædikat> er valgfrit, og kan indeholde en forkortelse, kaldenavn eller lignede for det system, brugersystemrollen er oprettet til. Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <It-system prædikat> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
  - <filternavn> Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <filter> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
  - <version> skal være et heltal mellem 1 og 99.
- EntityId for typen SEB: Udfyld med oplysninger om Systemnavn og Rollenavn. Det unikke entityId for brugersystemrollen skabes ud fra disse oplysninger og får følgende form: urn:dk:healthcare:[system-name]:[role-name] hvori de indtastede værdier vil være indsat.
- EntityId for typen NSP: Udfyld med oplysninger om Rollenavn. Det unikke entityId for brugersystemrollen skabes ud fra denne oplysning og får følgende form: urn:dk:healthcare:national-federation-role:[role-name] hvori den indtastede værdi vil være indsat.
- Dataafgræsningstyper: Denne mulighed gives kun for typerne KOMBIT og SEB. Du kan fremsøge dataafgrænsningstyper ved at søge i felterne Navn og Type. Vælg en dataafgrænsningstype ved at klikke på den i listen. Hvis der sættes flueben i Obligatorisk betyder det, at når myndigheden inkluderer brugersystemrollen i en jobfunktionsrolle, kræves det at pågældende dataafgrænsningstype udfyldes med en værdi. Afslut med at trykke "Opret".

Hvis brugersystemrollen ønskes slettet, kan det gøres ved at trykke på skraldespands-ikonet, som vises yderst til højre i listen af Brugersystemroller, herefter skal du bekræfte sletningen.





Oplysninger for et brugervendt system, der understøtter OIDC:



Udfyld følgende oplysninger på fanen Brugervendt system (OIDC-variant):

- Client ID: Offentlig identifikator for applikationen. Bruges af Context Handler til at genkende applikationen. Værdien skal være URI-formatteret (f.eks. https://example.com eller http://example.com).
- Client Type: Angiv om applikationen har typen ”public client” eller ”confidential client”. Dette har betydning for hvordan applikationen håndterer login og hemmelige nøgler.
    - "Public client" er typisk web- eller mobilapplikationer.
        - Dette valg indebærer, at Context Handler kommunikerer med klienten i henhold til OIDC-standardens indstillinger token_endpoint_auth_method = ”none” og application_type = ”javascript”
    - "Confidential client" er typisk backend-servere eller sikre apps
        - Dette valg indebærer, at Context Handler kommunikerer med klienten i henhold til OIDC-standardens indstillinger token_endpoint_auth_method = ” client_secret_post” og application_type = ”web”, og at der dermed også skal oprettes en Client Secret.
- Client Secret: Hemmelig nøgle brugt til at autentificere applikationen i flows, hvor der ikke er en bruger tilgængelig (f.eks. automatiserede jobs). Dette felt skal kun udfyldes, når Client Type er ”Confidential client”. Der er to muligheder:

- Du kan vælge at indtaste en værdi selv. Denne mulighed kan benyttes, hvis det brugervendte system allerede er konfigureret til en Client Secret, som herved kan benyttes i samspil med den fælleskommunale infrastruktur. Værdien skal være mindst 32 karakterer lang og må kun bestå af bogstaver (a-z, A-Z) og cifre (0-9).
- Du kan vælge at lade administrationsmodulet generere en værdi for Client Secret. I så fald skal du kopiere værdien og indsætte i konfigurationen for det brugervendte system. Kopiering kan ske ved at overføre værdien til computerens udklipsholder eller ved at få den vist og nedskrive den. Værdien bør holdes hemmelig for uvedkommende. Bemærk, at det ikke er muligt at få vist værdien for Client Secret for et allerede gemt system. Hvis værdien går tabt, skal du indtaste eller generere en ny og konfigurere det brugervendte system op med den nye værdi.



- Attributprofil: Valget af attributprofil afgør, hvilke brugeroplysninger der udstilles i tokens. Som standard vil et brugervendt system benytte attributprofilen "Fælleskommunal profil". Alternativt kan vælges ”Fælleskommunal Profil uden persondata”.
- Refresh tokens: Hvis du bruger "Refresh tokens" tillader du en bruger at forny sin adgangstoken uden at skulle logge ind igen.
- Login callback URL’er: En eller flere URL'er, hvortil brugeren sendes efter login. Skal præcist matche det, applikationen sender i OIDC-login-flowet.
- Logout callback URL: URL som brugeren sendes til efter log out. Bruges typisk til at rydde lokale sessioner i applikationen.
- Assurance level: Her angives det påkrævede sikkerhedsniveau for applikationen. Dette kan udtrykkes indenfor en af de to standarder NSIS eller NIST.
    - For NSIS er der følgende 3 sikkerhedsniveauer at vælge imellem:
        - Lav
        - Betydelig
        - Høj
    - For NIST er der følgende 4 sikkerhedsniveauer at vælge imellem:
        - Niveau 1 – Lille eller ingen tiltro til påstået identitet
        - Niveau 2 – Nogen tiltro til påstået identitet
        - Niveau 3 – Høj tillid til påstået identitet
        - Niveau 4 – Meget høj tillid til påstået identitet
- JWKS (JSON Web Key Set): En JWKS er en samling af offentlige nøgler, som bruges til at verificere login og tokens fra en ekstern identitetsudbyder. Ved at registrere en JWKS angiver du, hvilke nøgler systemet kan have tillid til. Du kan angive en JWKS på én af følgende to måder:
    1. Som en URI til en (typisk) well-known-adresse, der stiller en JWKS til rådighed
    2. Som et JSON-objekt

  Hvis den angives som en URI, skal adressen bruge HTTPS-protokollen.
- Frontchannel Logout callback URL: Her angives den URL, som brugeren automatisk sendes videre til, når der er logget ud. Front-channel logout anvendes kun for confidential web-klienter. Eksempel på en gyldig URL: https://app.example.dk/logout/frontchannel

- Backchannel Logout callback URL: Her angives den URL, systemet bruger i baggrunden til at give besked om, at en bruger er logget ud. Back-channel logout anvendes kun for confidential web-klienter. Eksempel på en gyldig URL: https://app.example.dk/logout/backchannel
- Brugersystemrolle: Virkemåden i sektionen for Brugersystemroller er den samme som for SAML-varianten. Der henvises til beskrivelsen ovenfor.

Skift af applikationstype fra SAML til OIDC:

Når et brugervendt system, der er gemt med applikationstypen SAML, åbnes for redigering, er det muligt at skifte applikationstypen til OIDC øverst på siden

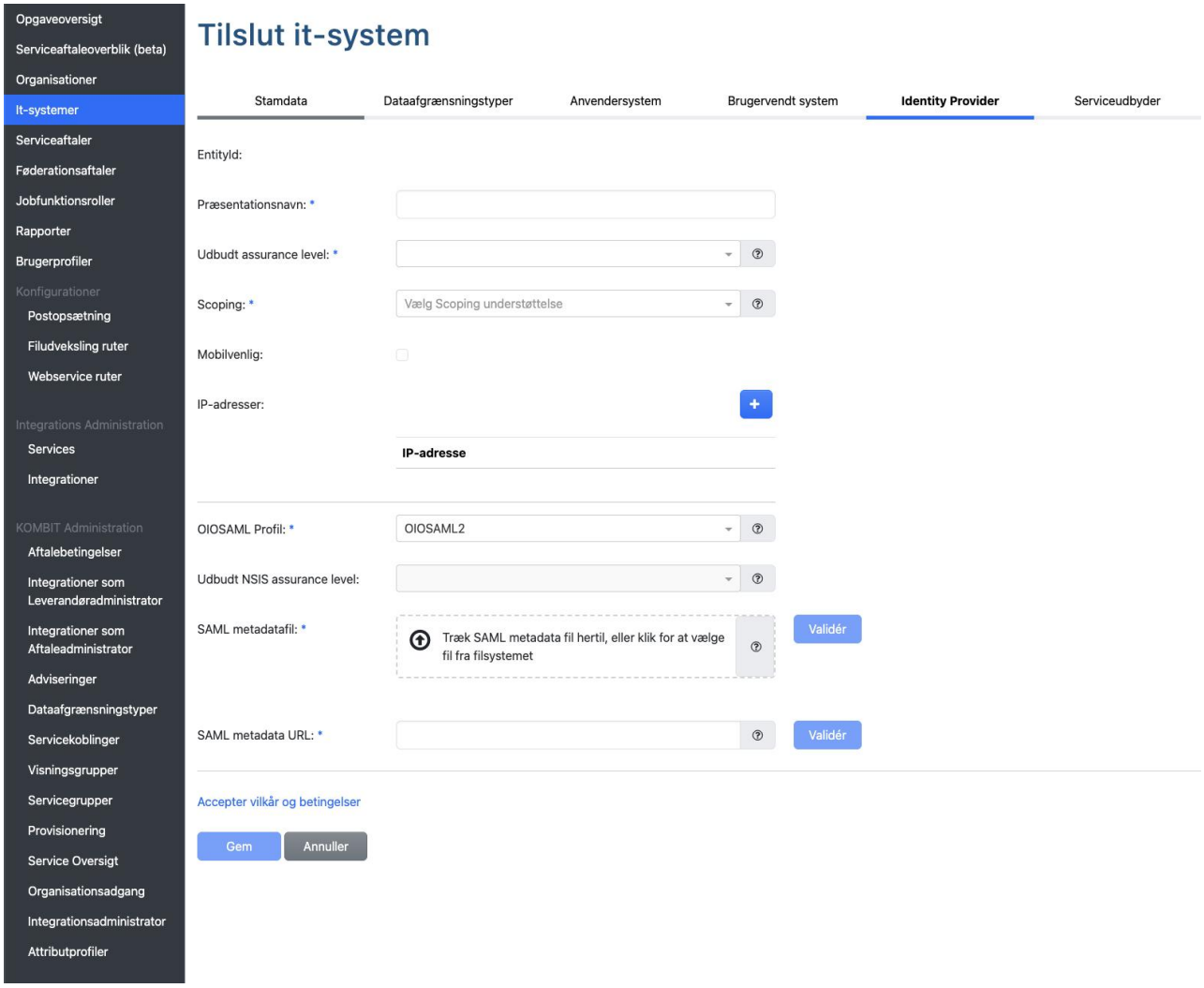


Når denne mulighed benyttes, vil Client ID være forudfyldt med EntityId fra SAML-typen. Dette kan overskrives med en URI-formatteret værdi efter eget ønske. Når først værdien er gemt, kan den dog ikke ændres efterfølgende.

Ligeledes vil allerede tilknyttede Brugersystemroller (og eventuelle rollemapninger af disse til Jobfunktionsroller) blive bibeholdt. Disse kan redigeres efter behov.

Indtastning af oplysninger for det brugervendte system følger i øvrigt beskrivelserne for OIDC-applikationstypen ovenfor.

5.7.5 Identity Provider



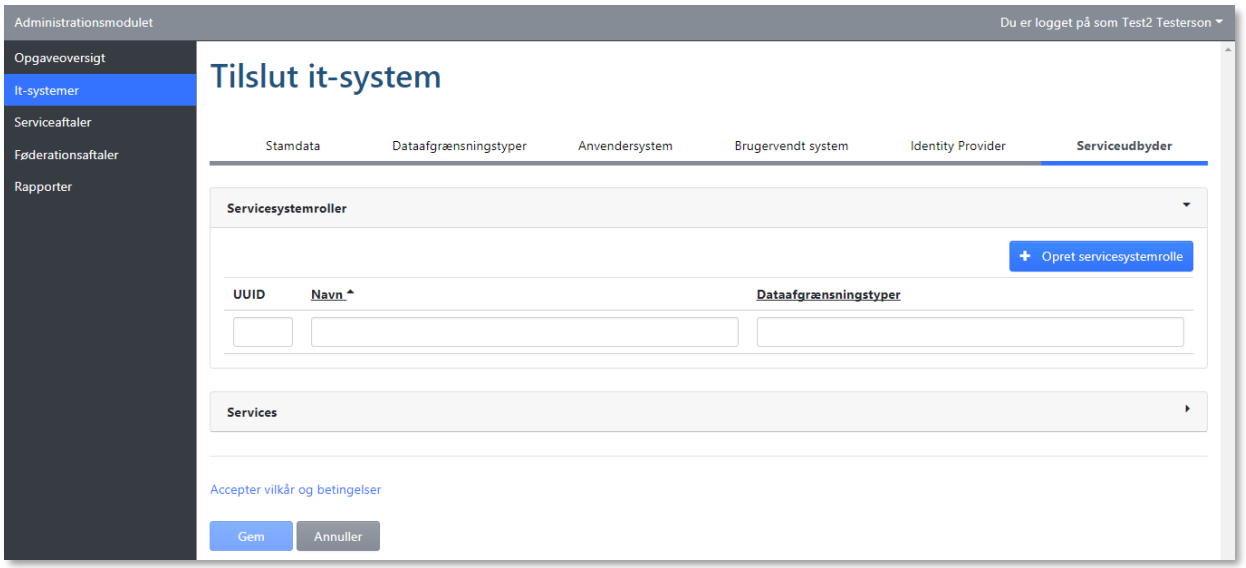
Udfyld følgende oplysninger på fanen Identity Provider:

- Præsentationsnavn: Her angives det navn som Context Handleren præsenterer brugerne for, når de skal vælge, hvilken Identity Provider, de vil logge på med.
- Udbudt assurance level:
    - Niveau 1 – Lille eller ingen tiltro til påstået identitet
    - Niveau 2 – Nogen tiltro til påstået identitet
    - Niveau 3 – Høj tillid til påstået identitet
    - Niveau 4 – Meget høj tillid til påstået identitet
- Scoping: Her angives information om hvorvidt Identity Provider understøtter Scoping. Scoping elementet anvendes til at informere Identity Provideren om identiteten af det Brugervendte System som brugeren er ved at logge på. Scoping for en Identity Provider kan derfor være en af følgende muligheder:
    - Understøtter ikke Scoping
    - Understøtter Scoping

Bemærk: Det er ikke alle IdP'er der understøtter scoping, så der er derfor vigtigt at undersøge om den registrerede IdP understøtter dette eller ej, inden dette element vælges til.

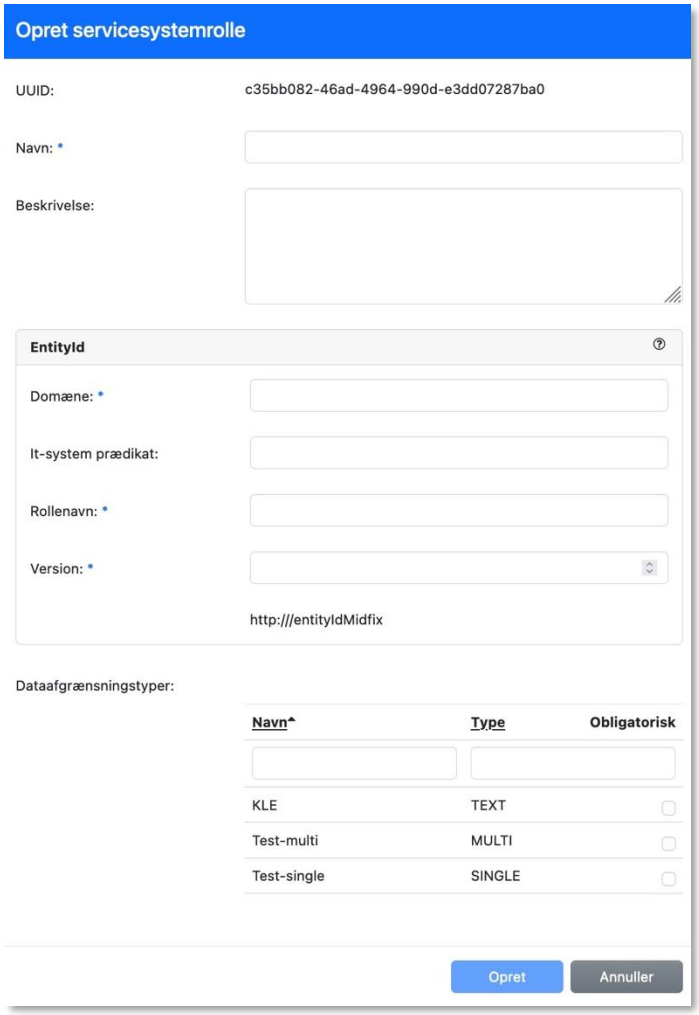
- Mobilvenlig: Markér feltet, hvis der er tale om en mobilvenlig Identity Provider der kan håndtere login via forskellige typer af mobilenheder.
- IP-adresser: Udfyldes hvis det kun er brugere fra bestemte IP-adresser, der må tilgå systemet. Det er muligt at tilføje flere ved at trykke på knappen med plus-ikonet.
- OIOSAML Profil: De mulige værdier er
    - OIOSAML2
    - OIOSAML2 - ADFS multipleauthn
    - OIOSAML2 - Without requested LoA
    - OIOSAML3
    - OIOSAML3 - ADFS multipleauthn
    - OIOSAML3 - ADFS relay state
- Ændring af OIOSAML Profil fra en OIOSAML2- til en OIOSAML3-profil er forbeholdt KOMBIT i Produktionsmiljøet, men kan administreres af leverandøren selv i ExtTest. Kontakt Serviceplatformens helpdesk, hvis profilen skal ændres fra en OIOSAML2- til en OIOSAML3-profil i Produktionsmiljøet. NSIS assurance level er inaktiv, hvis der ikke anvendes en OIOSAML3-profil.
- Udbudt NSIS assurance level: Ændring af NSIS assurance level for en Identity Provider er forbeholdt KOMBIT i Produktionsmiljøet men kan administreres af leverandøren selv i ExtTest. De mulige NSIS assurance levels er:
    - Lav
    - Betydelig
    - Høj
- SAML metadatafil: SAML metadatafilen indeholder blandt andet bindings og location for SAML services og it-systemets offentlige nøgle baseret på et Organisations- eller Systemcertifikat. Træk din SAML metadatafil ind på det markerede område, hvorefter den bliver indlæst. Alternativt kan der angives en SAML metadata URL.
    - SAML metadatafilen bliver valideret af Context Handler, inden den kan gemmes og benyttes. Hvis metadatafilen indeholder fejl, kan systemet ikke gemmes. Det anbefales, at du efter upload aktiverer knappen 'Validér'. Herved sendes filen til validering hos Context Handler, og eventuelle fejl (blokerende for gemning) og advarsler (ikke-blokerende) vil blive vist, så du har mulighed for at tilrette og uploade på ny.
- SAML metadata URL: I stedet for at uploade en SAML metadatafil, kan man angive en URL, hvor metadata kan hentes fra. URL'en skal være valid, og skal derudover være med https protokol. Der er samme krav til indholdet af metadata, som hvis den blev uploadet direkte på Administrationsmodulet.
    - SAML metadata-URL'en bliver valideret af Context Handler, inden den kan gemmes og benyttes. Context Handler hjemhenter metadatafilen ved at kalde metadata-URL'en, og hvis URL'en er utilgængelig eller den hjemhentede metadatafil indeholder fejl, kan systemet ikke gemmes. Det anbefales, at du efter indtastning af URL'en aktiverer knappen 'Validér'. Herved sendes URL'en til validering hos Context Handler, og eventuelle fejl (blokerende for gemning) og advarsler (ikke-blokerende) vil blive vist, så du har mulighed for at rette manglerne. Dette kan indebære tilpasninger til den service, som metadata-URL'en henviser til.

5.7.6 Serviceudbyder



På fanen Serviceudbyder kan du tilknytte eksisterende Servicesystemroller og Services eller du kan oprette nye Servicesystemroller og Services.

Servicesystemroller: For at oprette en ny servicesystemrolle tryk på knappen ”Opret servicesystemrolle” (bemærk, at de servicesystemroller der oprettes, skal svare til de servicesystemroller som systemet kan håndhæve).



Udfyld følgende oplysninger om Servicesystemroller:

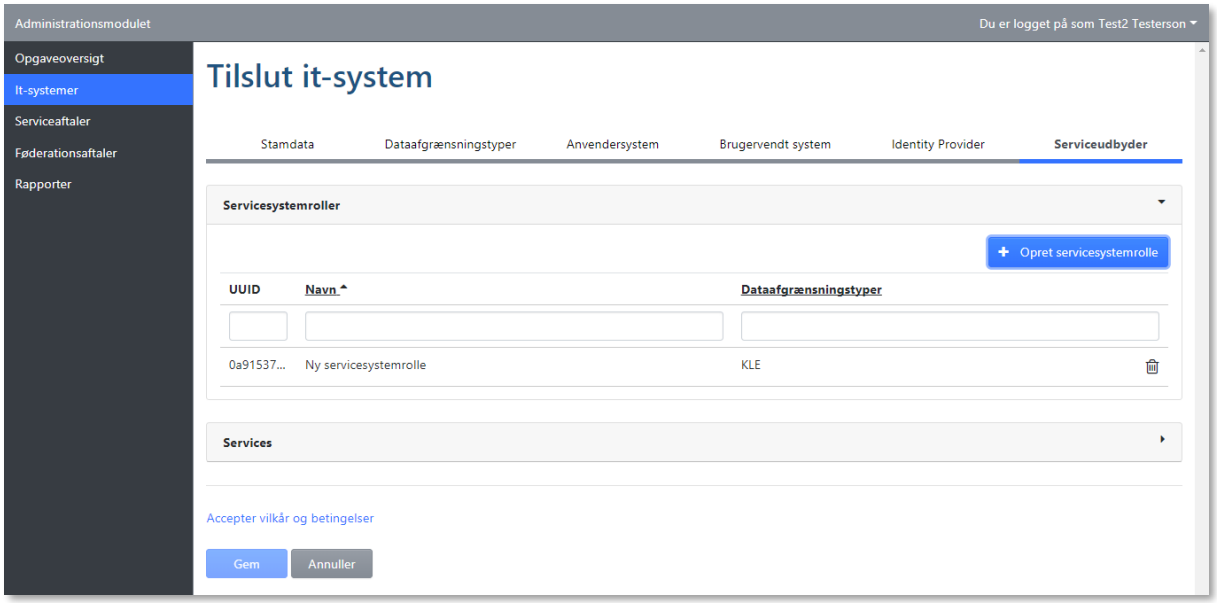
- Navn: Giv servicesystemrollen et sigende navn
- Beskrivelse: Tilføj en beskrivelse (er valgfrit at udfylde). Det anbefales at feltet udfyldes.
    - EntityId: Udfyld med oplysninger om Domæne, It-system prædikat (Valgfrit), Filternavn og Version.
      Det unikke navn for servicesystemrollen skabes ud fra disse oplysninger og får følgende form: http://<Domæne>/servicesystemrole/<It-system prædikat>/<Rollenavn>/<Version>. Det kunne eksempelvis være http://entityid.kombit.dk/servicesystemrole/bfo/aflever/1, hvor ’bfo’ angiver Beskedfordeler.
    - <domæne> skal bestå af mindst to led adskilt med punktum, hvert led skal bestå af mindst to tegn, hvor tilladte tegn er a-z, A-Z, 0-9 samt bindestreg og underscore, dog må første tegn i et led ikke være bindestreg eller underscore.

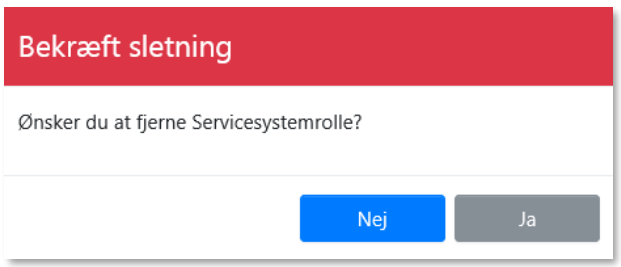
- <It-system prædikat> er valgfrit, og kan indeholde en forkortelse, kaldenavn eller lignede for det system, servicesystemrollen er oprettet til. Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <It-system prædikat> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
- <filternavn> Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <filter> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
- <version> skal være et heltal mellem 1 og 99.

- Dataafgræsningstyper: Du kan fremsøge dataafgrænsningstyper ved at søge i felterne Navn og Type. Vælg en dataafgrænsningstype ved at klikke på den i listen. Hvis der sættes flueben i Obligatorisk betyder det, at dataafgrænsningen skal udfyldes med en værdi på aftaleindgåelsestidspunktet. Hvis der ikke bliver vist nogle dataafgrænsningstyper, er det fordi, der ikke er blevet oprettet nogle endnu. Se punkt hvor fanen 5.7.2 Dataafgrænsningstyper forklares.

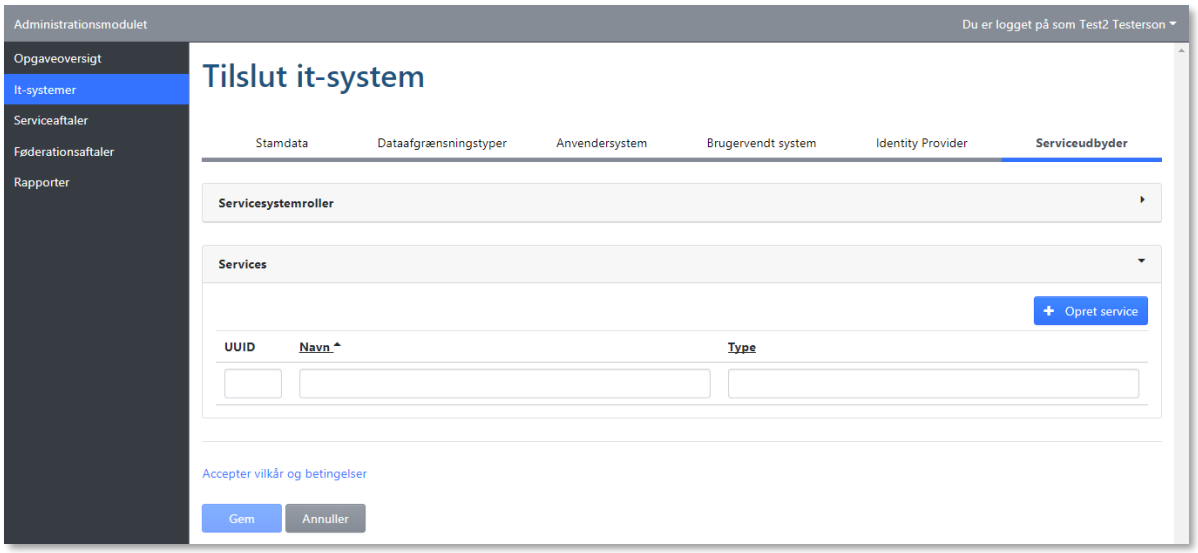
Afslut med at trykke ”Opret”.

Hvis servicesystemrollen ønskes slettet, kan det gøres ved at trykke på skraldespands-ikonet, som vises yderst til højre i listen af Servicesystemroller, herefter skal du bekræfte sletningen.



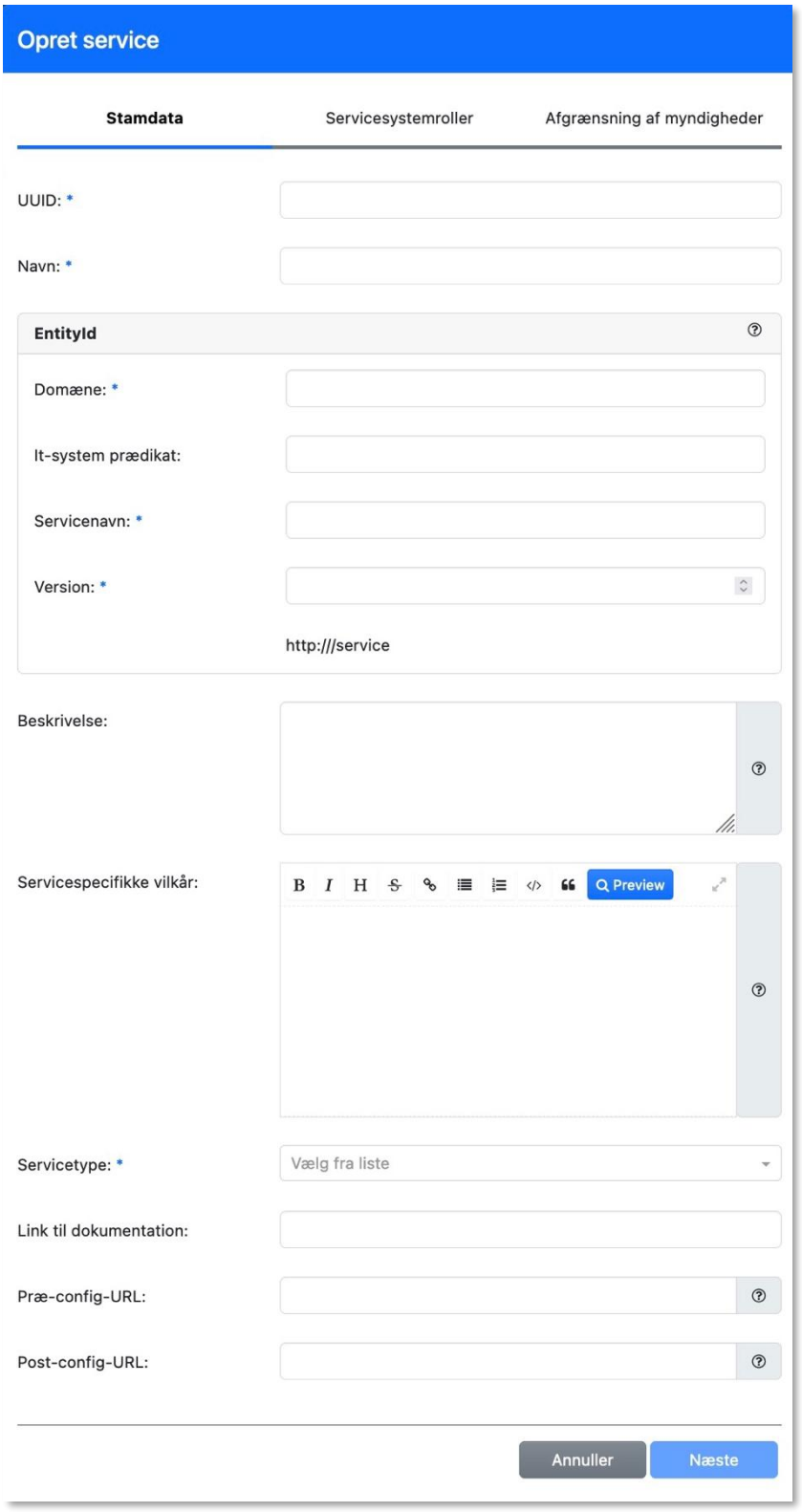


Services: For at oprette en ny service tryk på knappen ”Opret service” (bemærk at de services der oprettes, skal svare til de services som systemet udstiller).



For at oprette en ny service skal du igennem tre trin: Stamdata, Servicesystemroller og Afgrænsning af myndigheder.

1. Stamdata

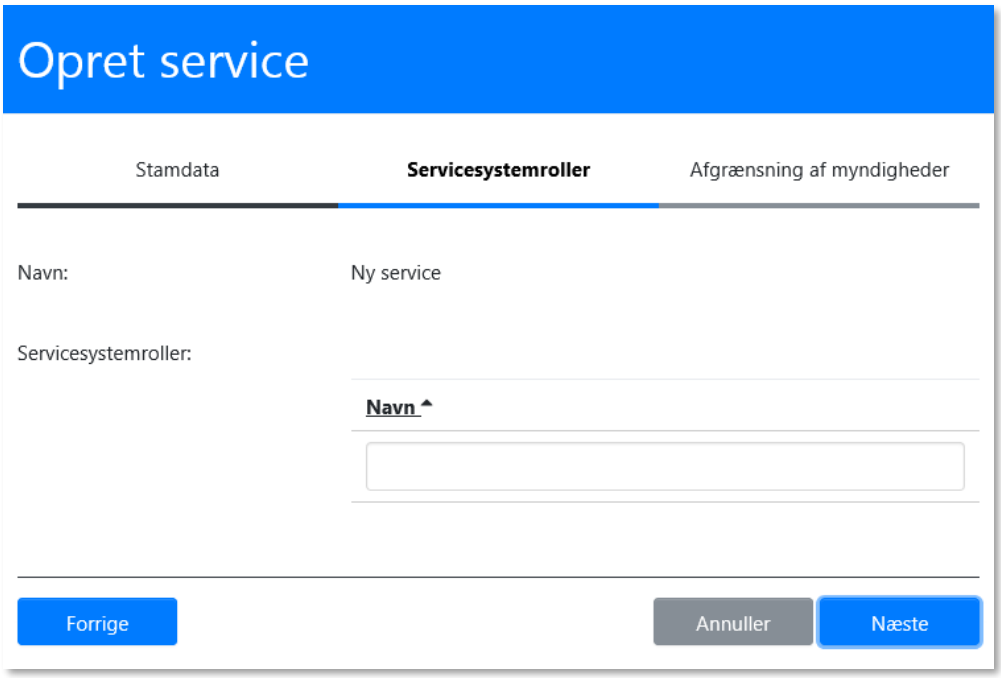


Udfyld følgende oplysninger om Stamdata:

- Navn: Giv servicen et sigende navn
- EntityId: Udfyld med oplysninger om Domæne, It-system prædikat, Filternavn og Version. Det unikke navn for servicen, som skal skrives på formen er: http://<Domæne>/service/<It-

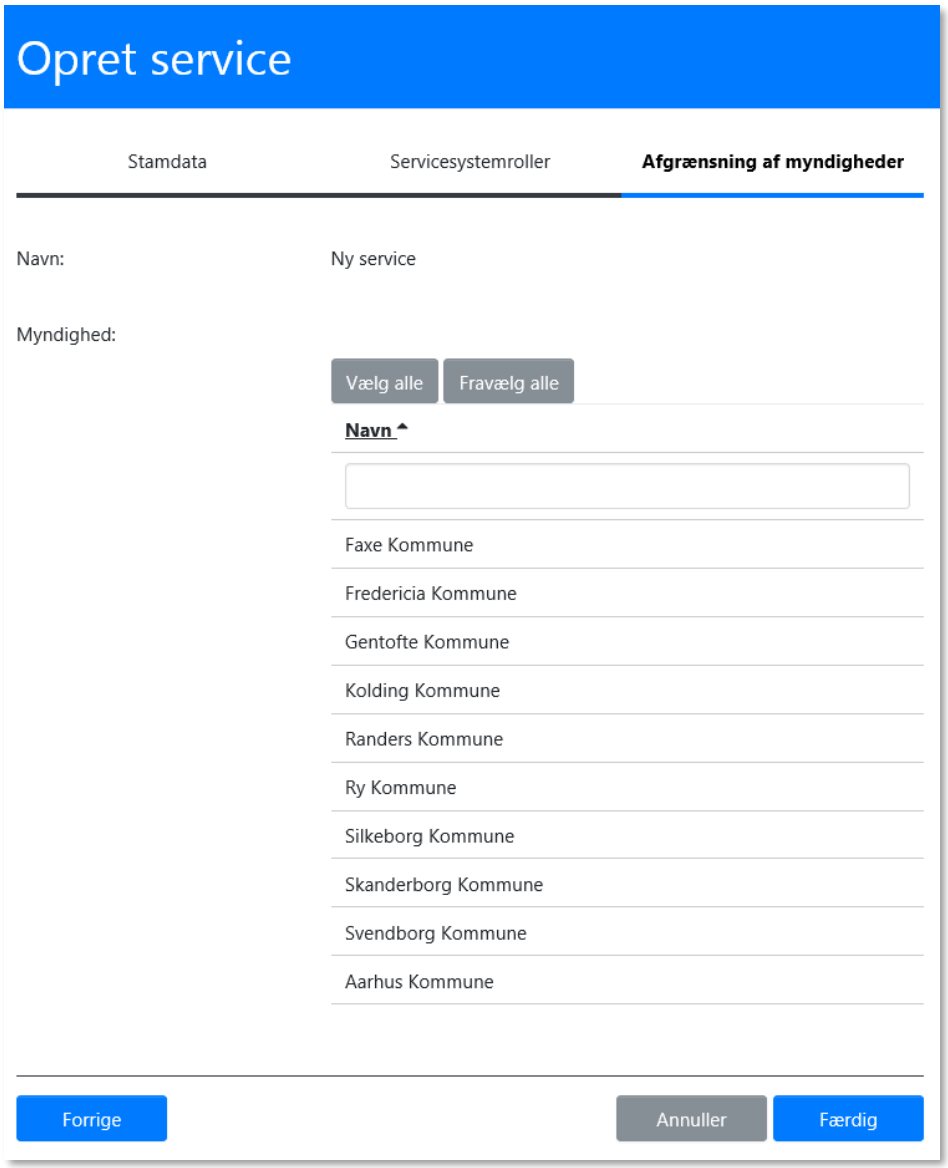
system prædikat>/<Servicenavn>/<Version>. Det kunne eksempelvis være http://entityid.kombit.dk/service/sp/eindkomst/3, hvor 'sp' angiver Serviceplatformen.
    - <domæne> skal bestå af mindst to led adskilt med punktum, hvert led skal bestå af mindst to tegn, hvor tilladte tegn er a-z, A-Z, 0-9 samt bindestreg og underscore, dog må første tegn i et led ikke være bindestreg eller underscore.
    - <It-system prædikat> er valgfrit, og kan indeholde en forkortelse, kaldenavn eller lignede for det system, servicen er oprettet til. Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <It-system prædikat> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
    - <filternavn> Her tillades a-z, A-Z, 0-9 samt bindestreg og underscore. <filter> skal indeholde mindst 2 tegn; dog må første tegn ikke være bindestreg eller underscore.
    - <version> skal være et heltal mellem 1 og 99.
- Beskrivelse: Tilføj en kort beskrivelse om de data servicen udstiller (KOMBIT anbefaler at man her skriver SF-nummeret på servicen)
- Servicespecifikke vilkår: Tilføj eventuelle servicespecifikke vilkår. Vilkårene vil indgå i de samlede vilkår som myndigheden skal acceptere ved godkendelse af serviceaftale på den pågældende service.
- Servicetype:
    - Simpel Service
    - Simpel Filtransport
    - Simpel Callback Service
    - Simpel Fælleskommunal Service
    - Fælleskommunal Service
    - Filservice med rutning
- Handling (vises kun ved valg af servicetypen "Filservice med rutning"): Afgør om det er Datamodtager eller Dataejer som skal godkende, hvis servicen bruges i en serviceaftale. (Handling og InfRef skal udgøre et unikt par)
- InfRef (vises kun ved valg af servicetypen "Filservice med rutning"): InfRef er en reference til feltet InfRef som står i den trigger fil der af anvender systemet skal leveres sammen med filen, InfRef benyttes til at koble den sendte fil sammen med serviceaftalen. (Handling og InfRef skal udgøre et unikt par).
- Videregivelse af data (vises kun ved valg af servicetypen "Fælleskommunal Service" eller "Filservice med rutning"): Tilføj flueben hvis samme Serviceaftale-entitet skal kunne kobles til flere Myndigheder via Aftalerelationen.
- Pre-config-URL: Tilføj pre-config URL, hvis der er behov for at leverandøren af anvendersystemet laver yderligere konfigurationer inden den udbudte service kan tages i brug.
- Post-config-URL: Tilføj post-config URL, hvis der er behov for at de myndigheder, hvis data der er udbudt af den givne service, laver yderligere konfigurationer inden den udbudte service kan tages i brug.

2. Servicesystemroller



Du kan fremsøge en servicesystemrolle ved at søge i feltet Navn. Vælg en servicesystemrolle ved at klikke på den fra listen.

3. Afgrænsning af myndigheder

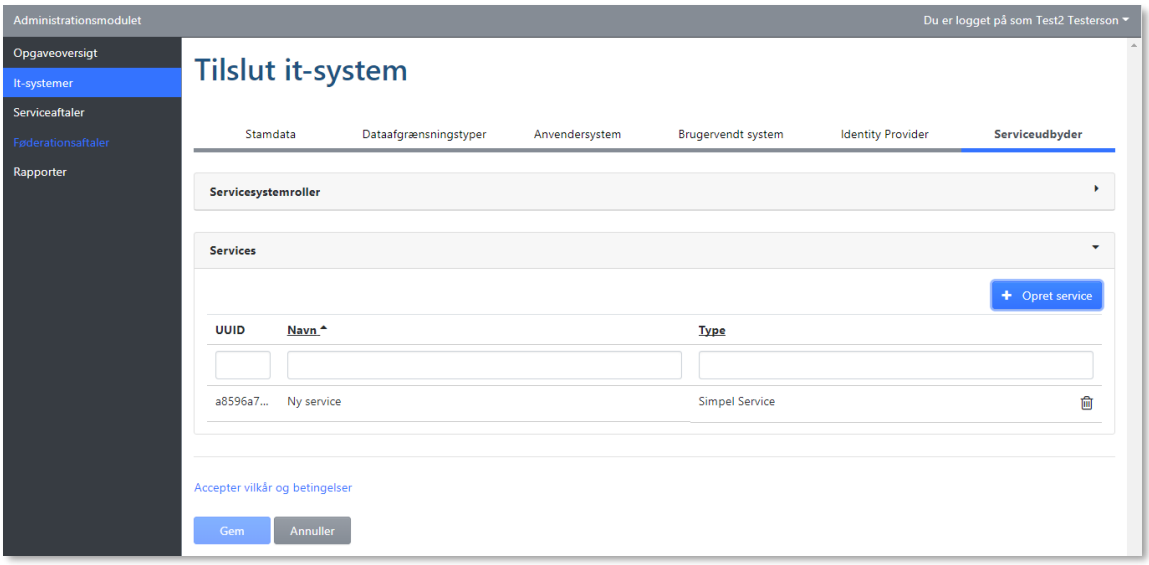


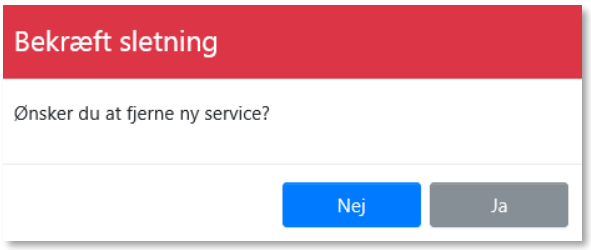
De myndigheder du tilføjer til denne liste, vil kunne indgå aftaler på servicen. Hvis du vælger ikke at tilføje nogle myndigheder, betyder det at alle myndigheder kan indgå aftaler på servicen inklusive myndigheder, der bliver oprettet fremadrettet. Hvis man omvendt vælger alle myndigheder, så vil det kun være de myndigheder, der står på listen ved oprettelse, som kan tilgå servicen, dvs. myndigheder som oprettes i Administrationsmodulet efterfølgende, vil ikke kunne tilgå servicen, men de kan tilføjes, hvis man redigerer servicen.

Du kan fremsøge en myndighed ved at søge i feltet Navn. Vælg en myndighed ved at klikke på den fra listen. Du kan også benytte knappen ”Vælg alle” til at vælge alle myndigheder, herefter kan du eventuelt fravælge enkelte myndigheder.

Når din service er færdigoprettet, trykker du på ”Færdig”.

Hvis servicen ønskes slettet, kan det gøres ved at trykke på skraldespands-ikonet, som vises yderst til højre i listen af Services, herefter skal du bekræfte sletningen.





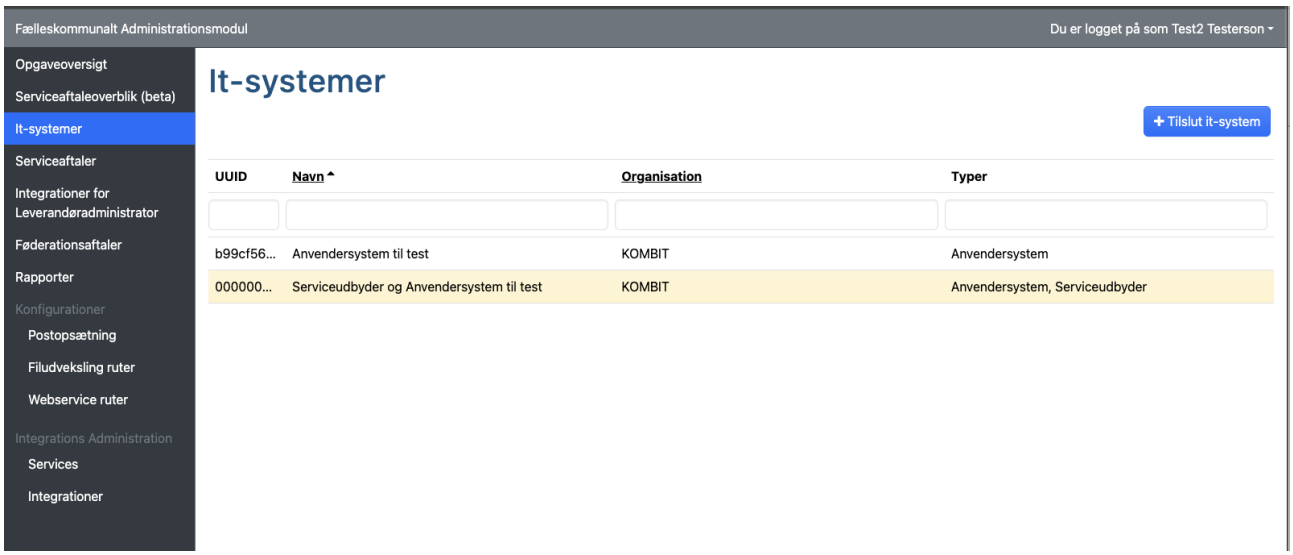
Resultat: Når du er færdig med at udfylde relevante faner under it-systemet, skal du afslutte med at trykke på linket ”Accepter vilkår og betingelser” i bunden af skærmbilledet, herefter kan du trykke ”Gem”, og du har nu oprettet et nyt it-system i Administrationsmodulet.

5.8 Rediger it-system

Brugeren: Med rollen Leverandøradministrator kan du redigere et it-system.

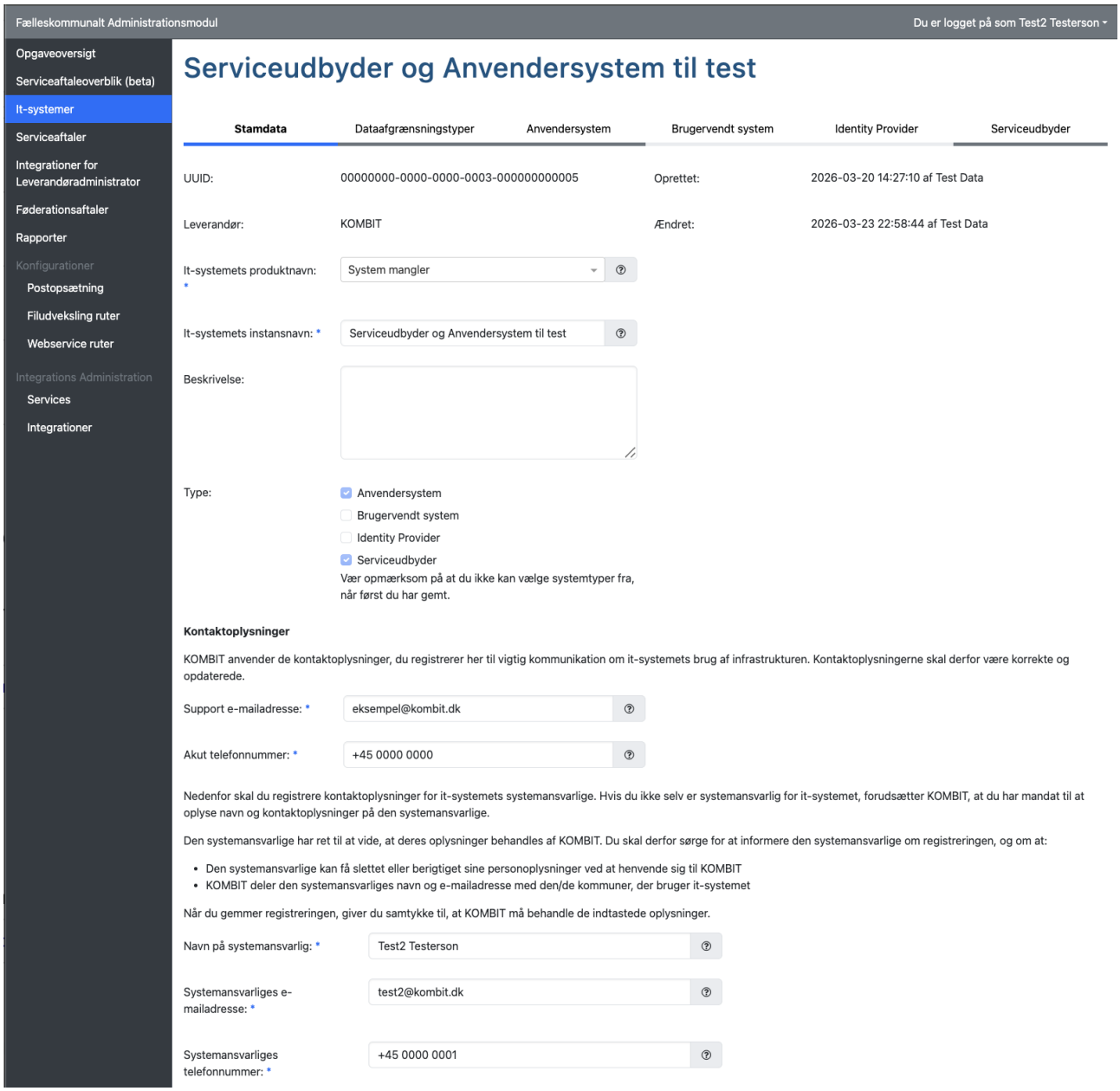
Vejledning:

1. I Administrationsmodulet skal du vælge punktet It-systemer i venstremenuen. Du kan fremsøge et it-system ved at søge i felterne UUID, Navn, Organisation og Type. Vælg et it-system fra listen ved at klikke på det.



2. Du kan nu redigere it-systemet.

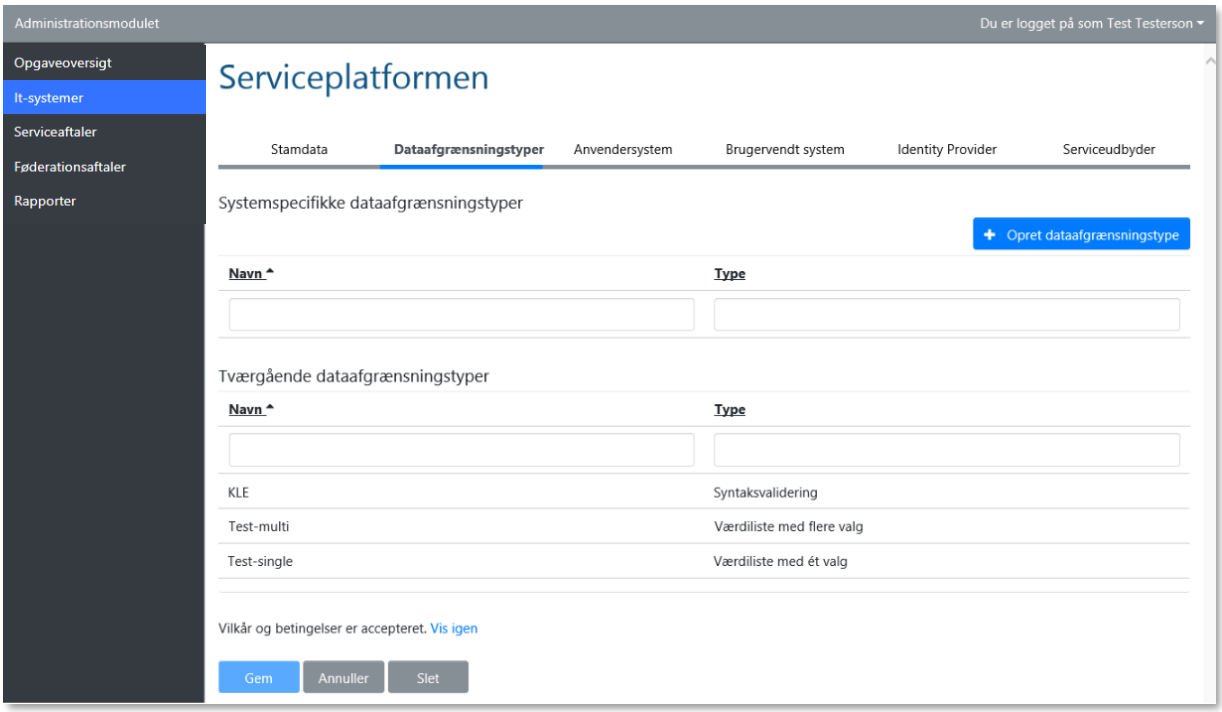
Stamdata



Under Stamdata kan du redigere:

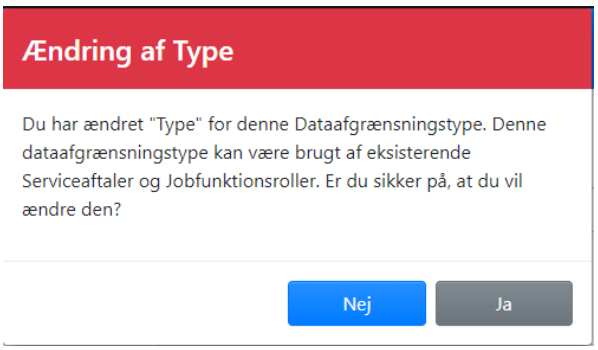
- It-systemets produktnavn
- It-systemets instansnavn
- Beskrivelse
- Type: Du kan tilføje systemtyper, men du kan ikke fravælge dem, der allerede er valgt.
- Kontaktoplysninger: Disse anvendes af KOMBIT til vigtig kommunikation om it-systemets brug af infrastrukturen. Kontaktoplysningerne skal derfor være korrekte og opdaterede. De omfatter:
    - Support e-mailadresse
    - Akut telefonnummer
    - Navn på systemansvarlig
    - Systemansvarliges e-mailadresse
    - Systemansvarliges telefonnummer

Dataafgrænsningstyper

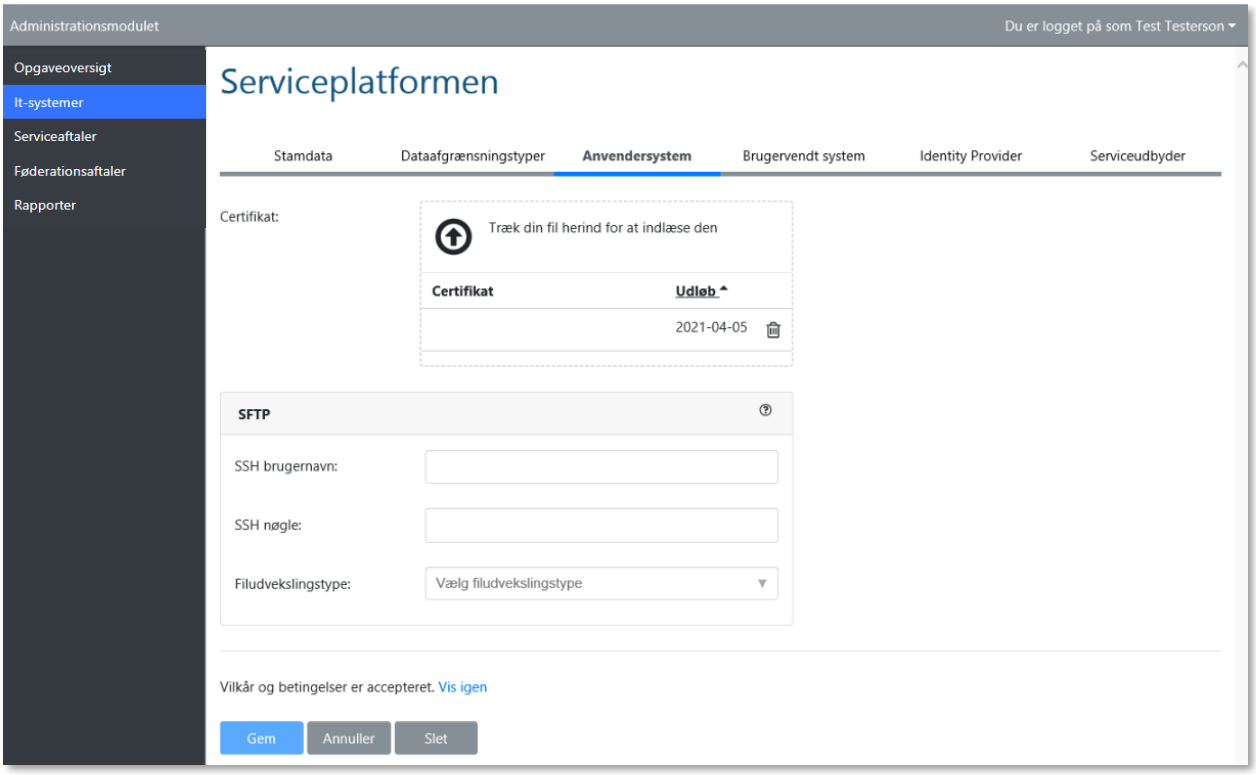


Under Dataafgrænsningstyper kan du:

- Oprette nye systemspecifikke dataafgrænsningstyper.
- Redigere systemspecifikke dataafgrænsningstyper. Bemærk at dataafgrænsningstyper kan være i brug på brugersystemroller og servicesystemroller som anvendes af hhv. jobfunktionsroller og services. Du kan ikke slette en dataafgrænsningstype, som er i brug på en systemrolle, den kan dog godt redigeres selvom den er i brug.
- Har du ændret typen på en dataafgrænsningstype, f.eks. fra Syntaksvalidering til Værdilistevalidering, skal dette bekræftes ved at svare på følgende dialog:



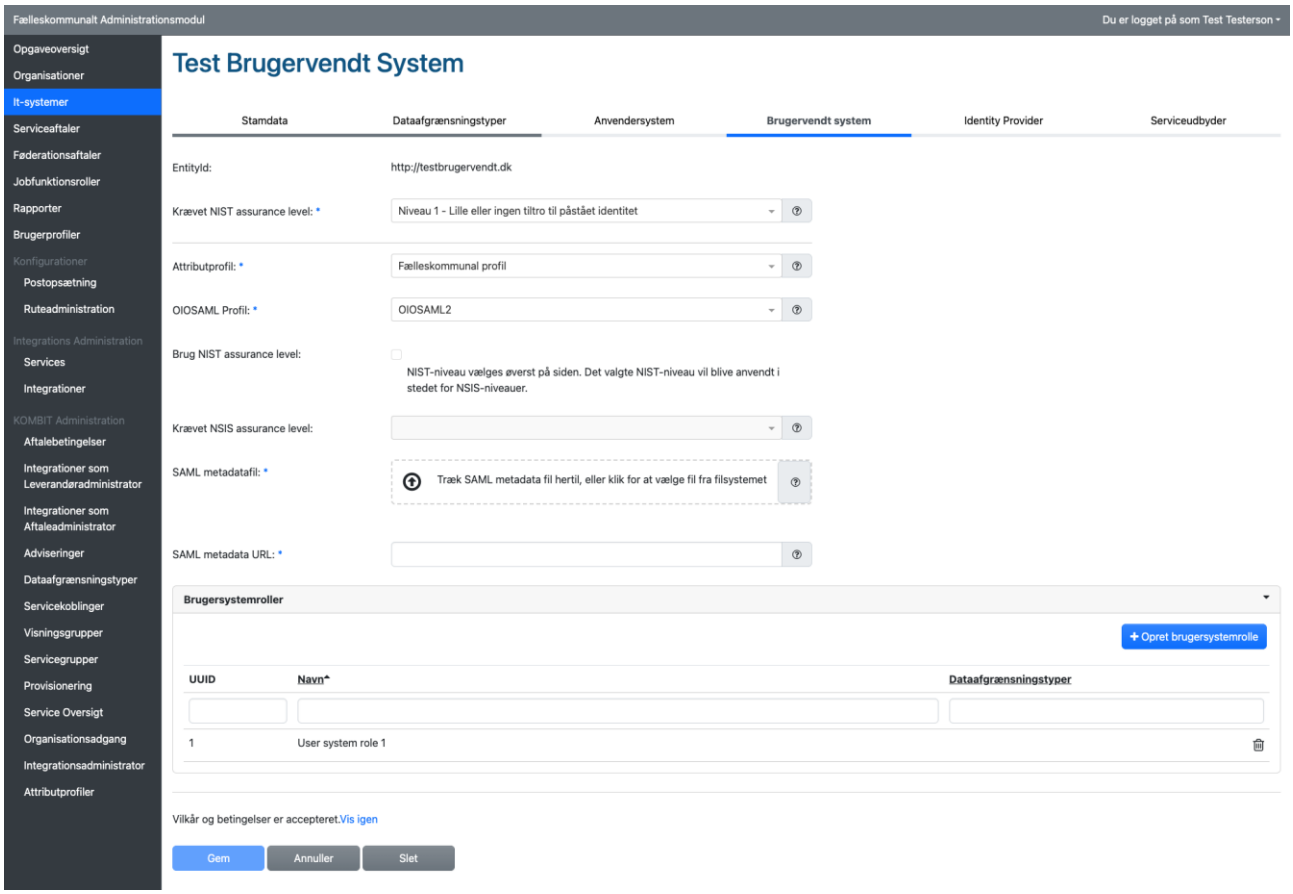
Anvendersystem



Under Anvendersystem kan du:

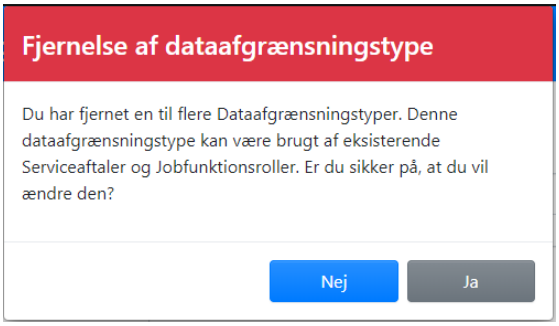
- Fjerne og tilføje certifikater, f.eks. hvis et eksisterende er ved at udløbe (bemærk at certifikatet skal være et base64 encoded X509-certifikat.). Der skal altid være mindst et certifikat, der er gyldigt. Samtlige certifikater bliver valideret, når et it-system gemmes.
- Redigere SFTP oplysninger.

Brugervendt system

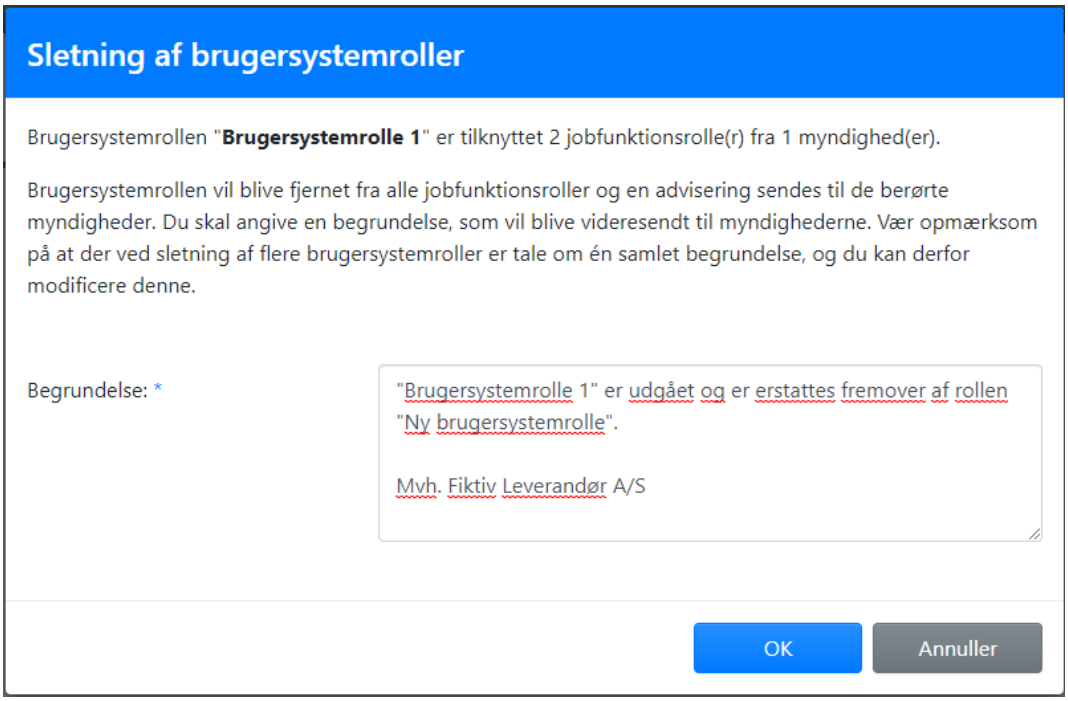


Under Brugervendt system kan du:

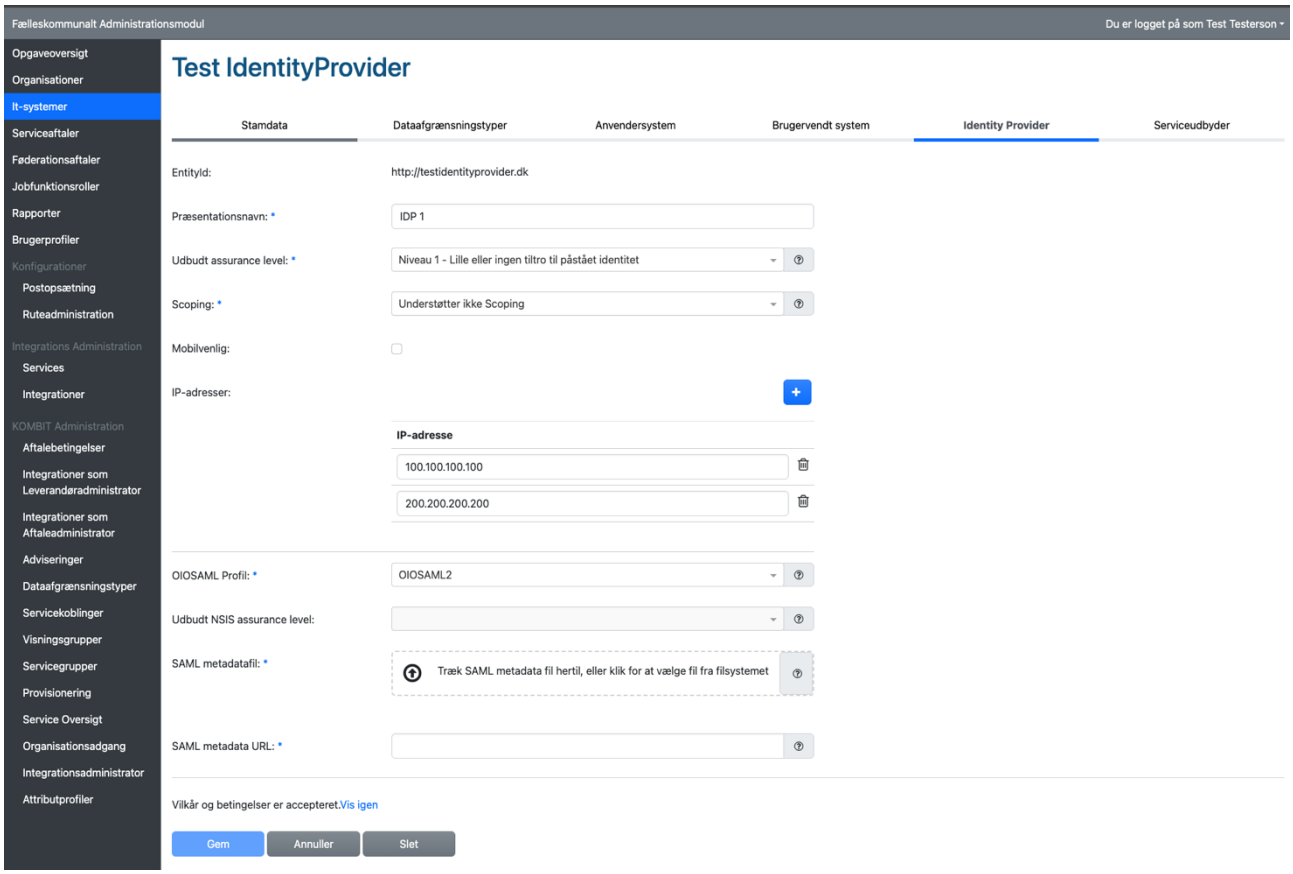
- Redigere krævet assurance level.
- Redigere understøttelse af Context Handler.
- Tilføje eller udskifte en SAML metadatafil f.eks. hvis en eksisterende er ved at udløbe. Der skal altid være en gyldig SAML metadatafil eller SAML metadata URL. SAML metadatafiler bliver valideret, når et it-system gemmes.
- Redigere OIOSAML Profil.
- Redigere krævet NSIS assurance level.
- Redigere SAML metadata URL.
- Tilføje en ny brugersystemrolle eller redigere en eksisterende brugersystemrolle. En brugersystemrolle med tilknyttede dataafgræsningstyper, kan være i brug på en jobfunktionsrolle. I dette tilfælde er det muligt at fjerne en eller flere dataafgrænsningstyper der er tilknyttet brugersystemrollen. Fjernelse af en dataafgrænsningstype fra en brugersystemrolle skal dog bekræftes ved følgende dialog når brugersystemrollen lukkes:



- Slette en brugersystemrolle. Såfremt brugersystemrollen ikke er i brug på jobfunktionsroller, kan den uden videre slettes fra det brugervendte system. Hvis brugersystemrollen er i brug på en eller flere jobfunktionsroller, vil du blive gjort opmærksom på dette ved nedenstående dialog. Hvis du accepterer konsekvenserne af sletningen (brugersystemrollen vil automatisk blive fjernet fra alle jobfunktionsrollerne) og vælger at fortsætte, skal du angive en begrundelse. De berørte myndigheder vil blive orienteret om sletningen i en advisering, som blandt andet indeholder din begrundelse.



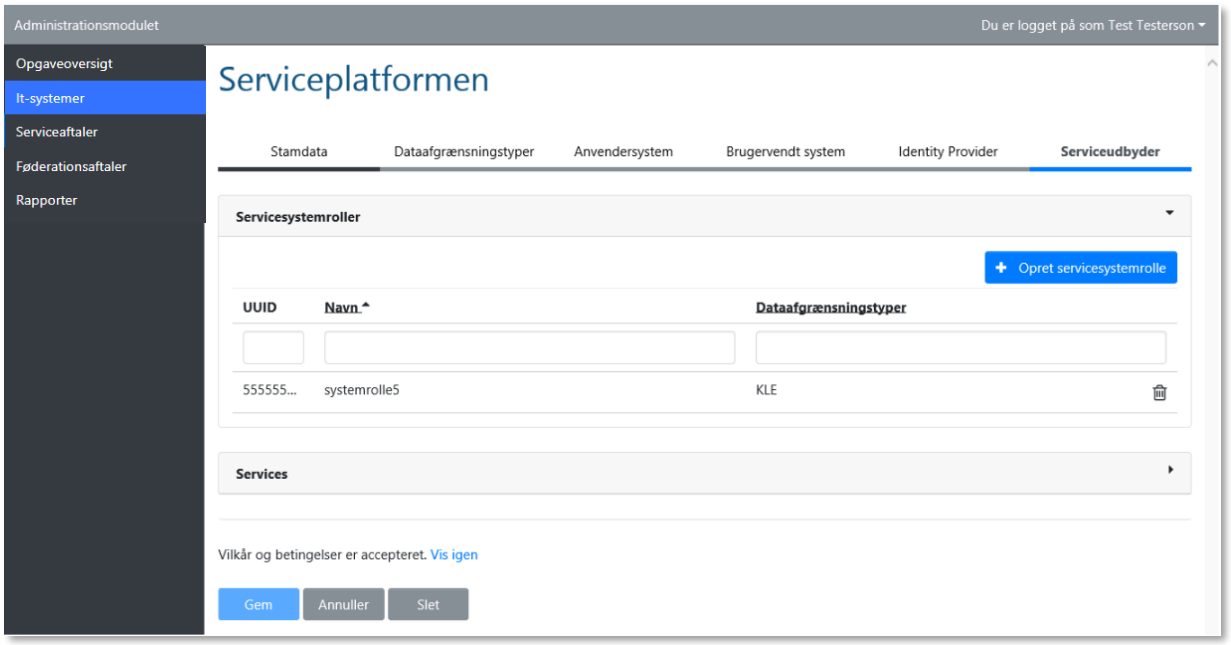
Identity Provider



Under Identity Provider kan du:

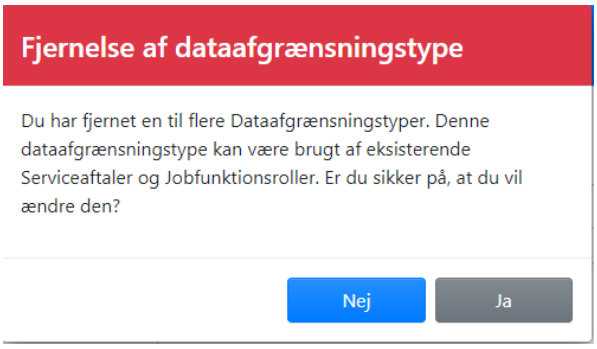
- Redigere præsentationsnavn.
- Redigere udbudt assurance level.
- Redigere Scoping understøttelse.
- Tilvælge mobilvenlig, hvis det er relevant.
- Fjerne eller tilføje IP-adresser.
- OIOSAML Profil: Her kan vælges blandt følgende værdier. I Produktionsmiljøet skal en KOMBIT-administrator dog godkende og åbne for OIOSAML3-profilerne:
  - OIOSAML2
  - OIOSAML2 - ADFS multipleauthn
  - OIOSAML2 - Without requested LoA
  - OIOSAML3
  - OIOSAML3 - ADFS multipleauthn
  - OIOSAML3 - ADFS relay state
- Udbudt NSIS assurance level: Skal vælges, hvis OIOSAML Profil er en af typerne startende med OIOSAML3.
- Tilføje eller udskifte en SAML metadatafil hvis den eksisterende er ved at udløbe. Der skal altid være enten en gyldig SAML metadatafil uploadet eller en SAML metadata URL.
- Redigere SAML metadata URL.

Serviceudbyder



Under Serviceudbyder kan du:

- Tilføje en ny servicesystemrolle eller redigere en eksisterende servicesystemrolle. Bemærk, at en servicesystemrolle med tilknyttede dataafgrænsningstyper, kan være i brug på en service. Ved redigering af en servicesystemrolle, er det muligt at fjerne en eller flere dataafgrænsningstyper, ved at trykke på den pågældende dataafgrænsningstype, der ønskes fjernet. Dette skal dog bekræftes ved følgende dialog, når servicesystemrollen lukkes:



- Slette en servicesystemrolle, hvis den ikke er i brug på en service.
- Tilføje en ny service eller redigere en eksisterende service. Bemærk, at services kan være i brug på serviceaftaler. Du kan slette en service, hvis den ikke er i brug.

3. Afslut med at trykke ”Gem”. Hvis der findes opgaver relateret til it-systemet, som ikke er udført, vises en dialog, hvor det er muligt at markere opgaverne som udført. Se afsnit 5.6 punkt 4 for mere information.

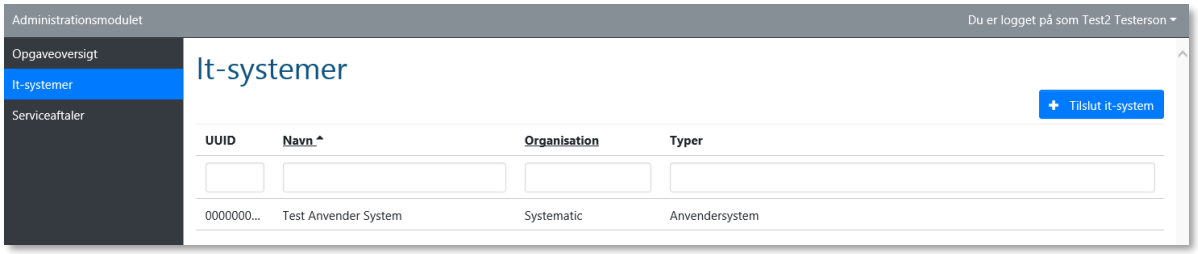
Resultat: Du har redigeret et it-system i Administrationsmodulet.

5.9 Slet it-system

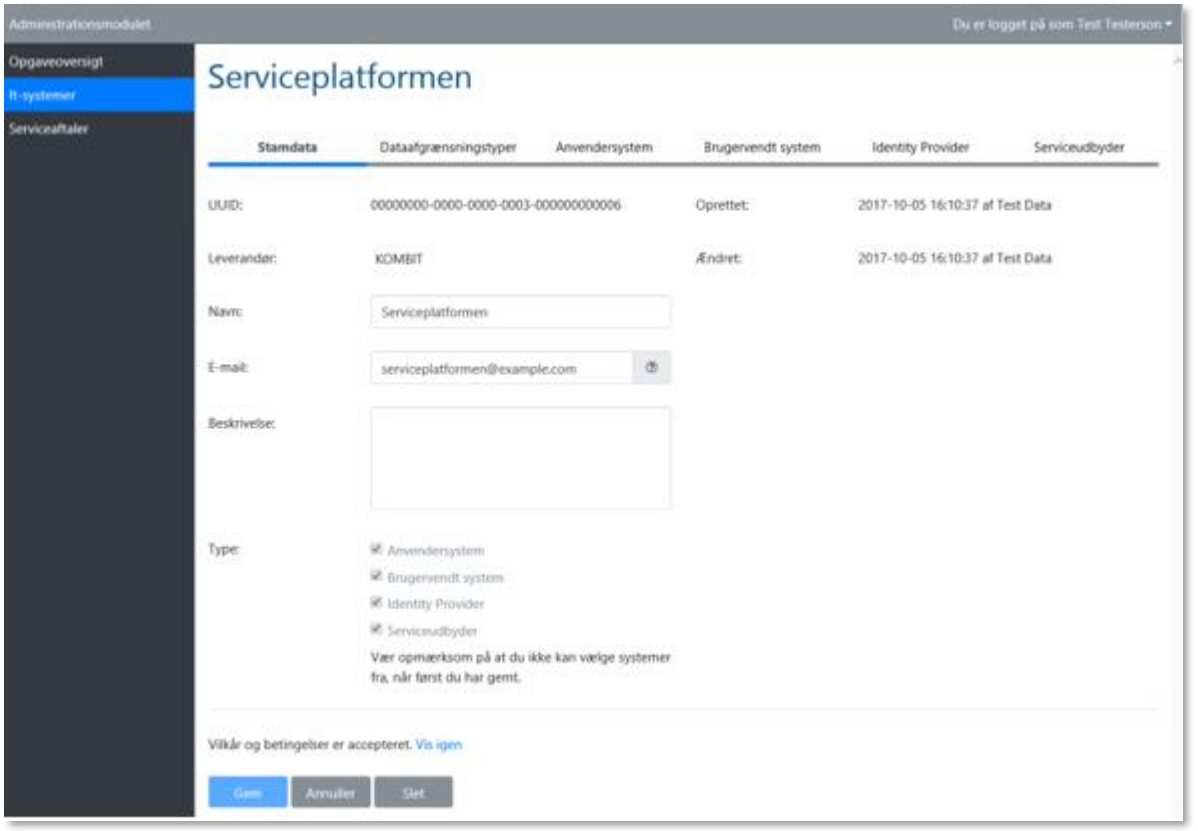
Brugeren: Med rollen Leverandøradministrator kan du slette et it-system.

Vejledning:

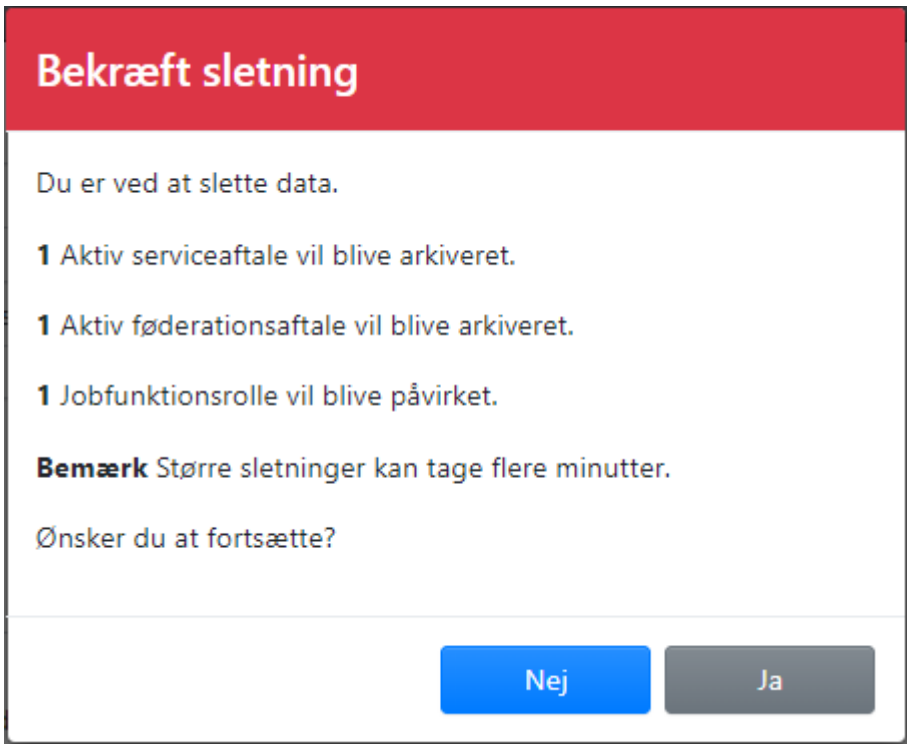
1. I Administrationsmodulet skal du vælge punktet It-systemer i venstremenuen. Du kan fremsøge et it-system ved at søge i felterne UUID, Navn, Organisation og Type. Vælg et it-system fra listen ved at klikke på det.



2. Du kan slette it-systemet ved at trykke på knappen ”Slet”.



Omfanget af sletningen præsenteres ved hjælp af følgende dialog:



Ved tryk på Ja, sker følgende:

- For anvendersystem arkiveres tilknyttede serviceaftaler og systemet fjernes fra eventuelle visningsgrupper.
- For brugervendt system fjernes alle brugersystemrollernes tilknytninger til jobfunktionsroller.
- For serviceudbyder arkiveres alle serviceaftaler, der benytter systemets udstillede services. Servicekoblinger fjernes, hvis services fra serviceudbyderen indgår heri.
- For identity provider arkiveres tilknyttede føderationsaftaler.

Resultat: Du har slettet et it-system i Administrationsmodulet, og det er ikke længere muligt at indgå aftaler med det pågældende it-system.

5.10 Skift af certifikat

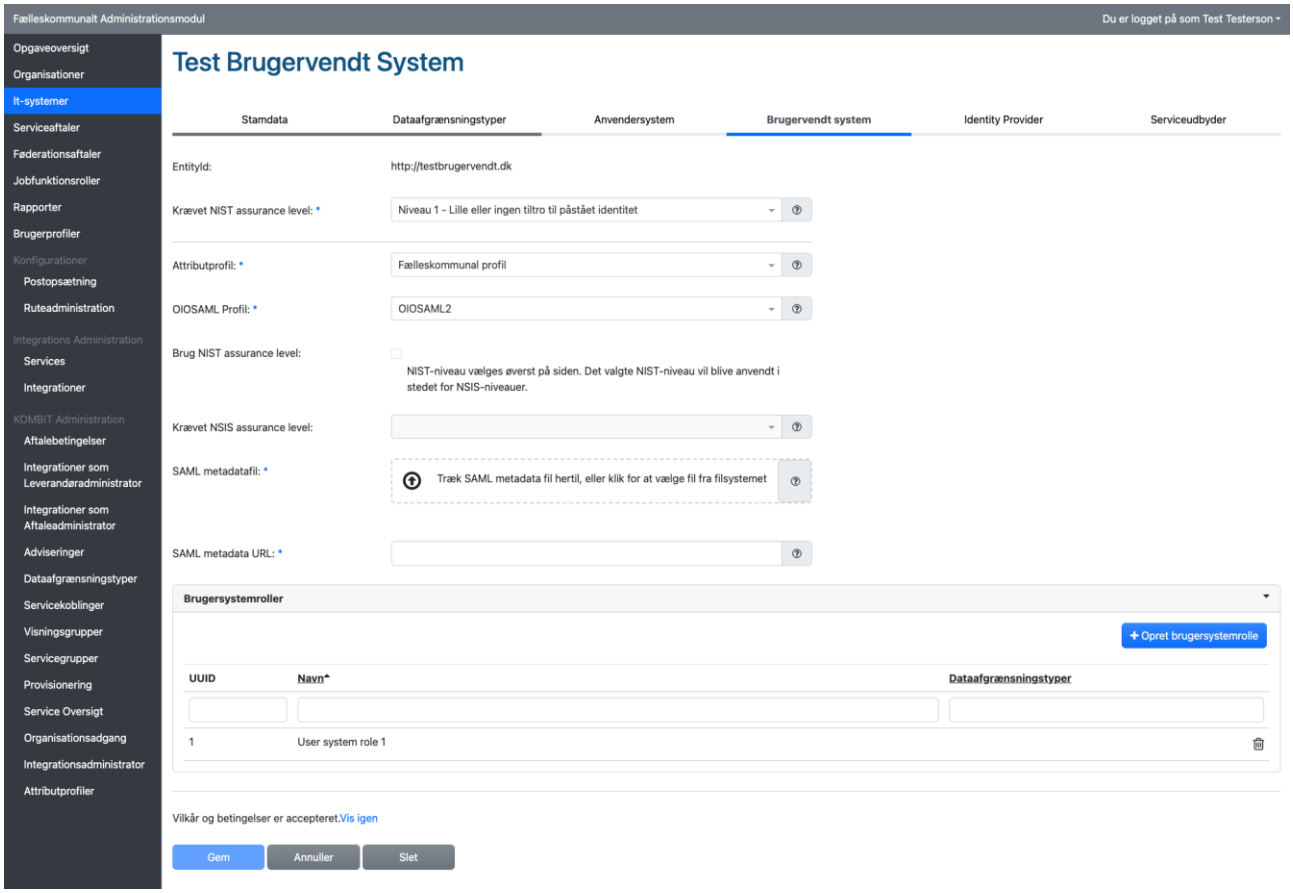
Alt efter hvilken type dit system er, skal du skifte certifikat på følgende måde.

5.10.1 Anvendersystem

Organisations- og Systemcertifikat.: Se afsnit 5.4.3
SSH: Se afsnit 5.4.3

5.10.2 Brugervendt System

Det certifikat et Brugervendt System anvender mod Adgangsstyring er indeholdt i de SAML metadata som er registreret i Administrationsmodulet. Når man skifter certifikatet i sit brugervendte system, skal der registreres nye SAML metadata i Administrationsmodulet, indeholdende det nye certifikat. Når SAML metadata er klar til registrering, skal man logge på Administrationsmodulet og navigere til det pågældende It-system, hvor man på fanen "Brugervendt System" kan uploade den nye SAML metadata fil.



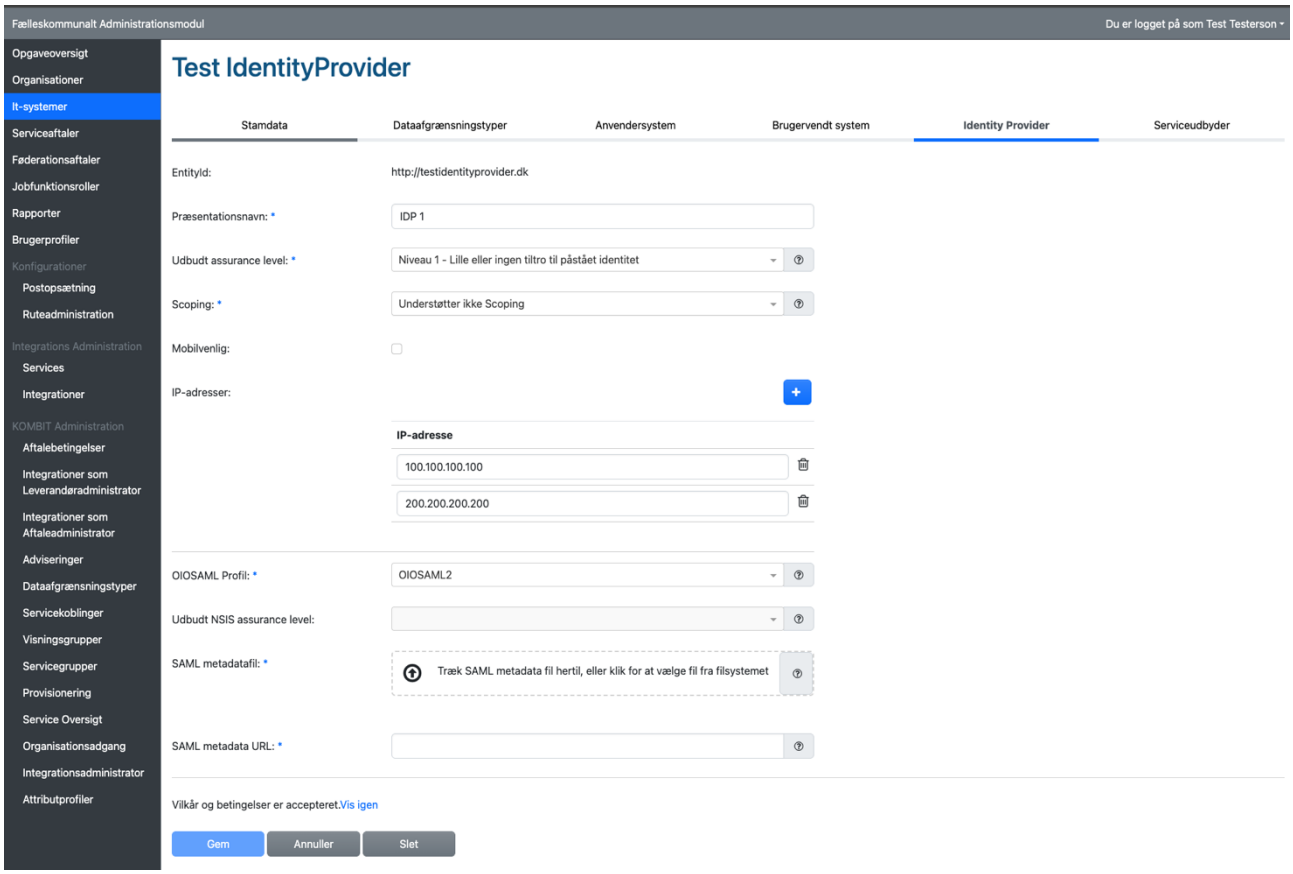
Herefter er det nye certifikat klar til brug med støttesystemet Adgangsstyring.

Bemærk, at man ikke kan registrere flere SAML metadata samtidig for et brugervendt system og ej heller registrere SAML metadata, der indeholder mere end ét certifikat. For at undgå nedetid i forbindelse med certifikatskifte på sit brugervendte system kan man anvende SAML metadata URL i stedet.

Identity Provider

Det certifikat en Identity Provider anvender mod Adgangsstyring er indeholdt i de SAML metadata som er registreret i Administrationsmodulet. Når man skifter certifikatet i sin Identity Provider, skal der registreres nye SAML metadata i Administrationsmodulet indeholdende det nye certifikat.

Når SAML metadata er klar til registrering, skal man logge på Administrationsmodulet og navigere til det pågældende It-system, hvor man på fanen ”Identity Provider” kan uploade den nye SAML metadata fil.



Herefter er certifikatet opdateret for Identity Provideren.

Bemærk, at man ikke kan registrere flere SAML metadata samtidig for en Identity Provider og ej heller registrere SAML metadata, der indeholder mere end ét certifikat. For at undgå nedetid i forbindelse med certifikatskifte på sin Identity Provider, kan man anvende SAML metadata URL i stedet.

5.10.3 Service Udbyder

Der er ikke nogen certifikater tilknyttet denne systemtype.

5.11 Anmod om en serviceaftale

Brugeren: Med rollen leverandøradministrator kan du anmode én eller flere myndigheder om at behandle deres data via en serviceaftale. Derved får din organisations it-system mulighed for at tilgå en eller flere services på vegne af myndigheden.

Bemærk: For at behandle en myndigheds data, skal der også være indgået en gyldig databehandleraftale. Databehandleraftaler er ikke understøttet af Administrationsmodulet.

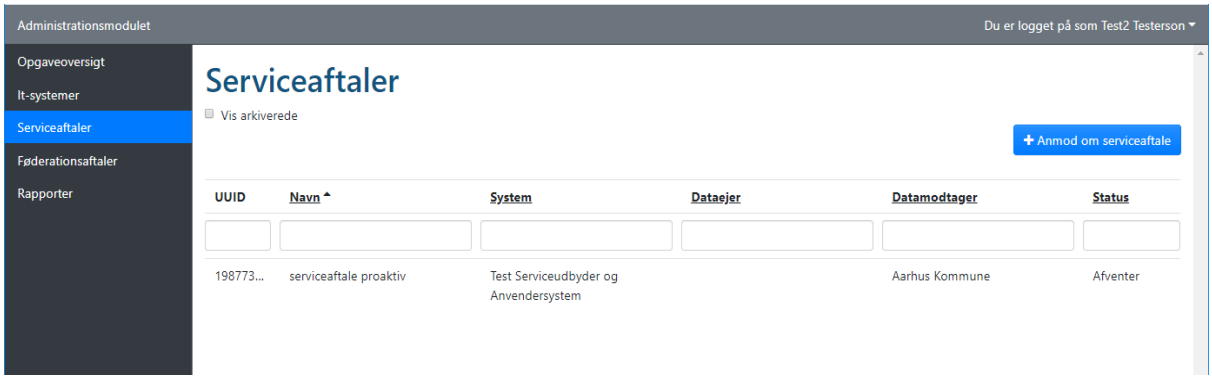
Man kan anmode om serviceaftale på to forskellige måder i Administrationsmodulet.

Den *'klassiske' fremgangsmåde*, hvor man som bruger selv skal træffe valg om, hvilke services, man ønsker adgang til, eller ved brug af *Integrationer*. Når man vælger fremgangsmåden ved brug af Integrationer, har en Integrationsadministrator på forhånd truffet valg om, hvilke services, der er relevante for den valgte type af integration, og Integrationsadministrator kan også have truffet valg om de detaljerede parametre.

5.11.1 Klassisk fremgangsmåde

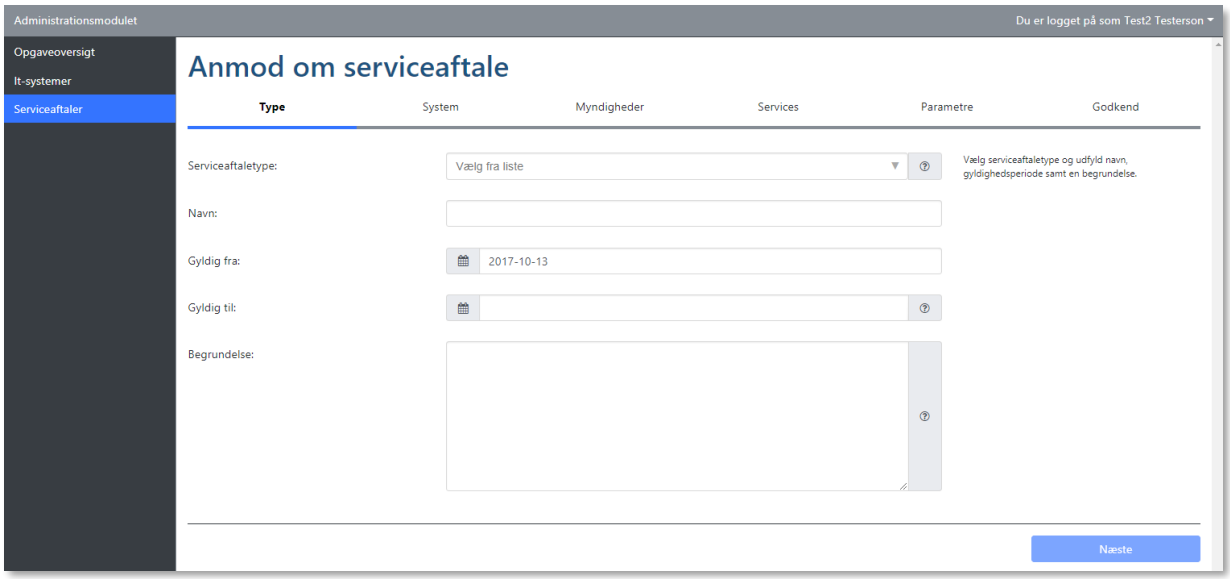
Vejledning:

I Administrationsmodulet skal du vælge punktet Serviceaftaler i venstremenuen. Herfra får du overblik over serviceaftaler der allerede er anmodet om. Du kan fremsøge en serviceaftale ved at søge i felterne UUID, Navn, System, Dataejer, Datamodtager og Status. Vælg serviceaftale ved at klikke på den fra listen.



For at anmode om en serviceaftale, skal du trykke på knappen "Anmod om serviceaftale". Herefter skal du igennem seks trin for at gennemføre anmodningen: Type, System, Myndigheder, Services, Parametre og Godkend.

1. Type



Udfyld følgende oplysninger om Type:

- **Serviceaftaletype**:
  - **Uden videregivelse af data (standardaftale):**
    Ved valg af denne aftaletype, betyder det, at du anmoder om én eller flere af myndigheders data
  - **Med videregivelse af data, flere datamodtagere:**
    Ved valg af denne aftaletype, betyder det, at du på vegne af flere myndigheder tilgår én myndigheds data
  - **Med videregivelse af data, flere dataejere:**
    Ved valg af denne aftaletype, betyder det, at du på vegne af én myndighed tilgår flere myndigheders data
  - **Med videregivelse af data, én dataejer og én datamodtager:**
    Ved valg af denne aftaletype, betyder det, at du på vegne af én myndighed tilgår én anden myndigheds data
- **Navn**: Giv serviceaftalen et sigende navn. Bemærk dette skal være unikt for det pågældende anvendersystem kombineret med datamodtager og dataejer.
  - ***Retningslinjer**: Ved navngivningen af en serviceaftale skal navnet som minimum indeholde snitflade id (SFxxxx) eller navnet på den service der bruges og versionen af servicen hvis dette er relevant.*
- **Gyldig fra**: Udfyld hvornår aftalen skal være gyldig fra.
- **Gyldig til**: Udfyld hvornår aftalen skal være gyldig til.
  - ***Retningslinjer for eksternt testmiljø**: Som udgangspunkt bør gyldighedsperioden for en serviceaftale være højst 1 år. Hvis en serviceaftale ikke har en gyldighedsperiode, bliver denne sat til 3 måneder i forbindelse med godkendelse med mindre andet er aftalt.*
  ***Retningslinjer for produktionsmiljøet**: Gyldighedsperioden ved oprettelse af en serviceaftale skal aftales mellem leverandør og myndighed i forbindelse med at det relevante IT-systems produktionssættes.*
- **Begrundelse**: Tilføj begrundelse for anmodningen om serviceaftalen. Begrundelsen ses når myndigheden skal godkende anmodningen.

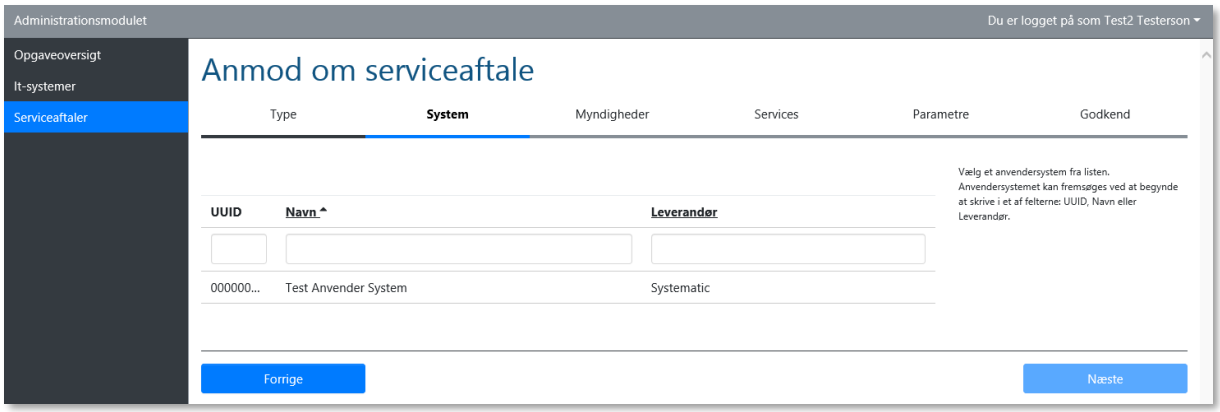
- ***Retningslinjer**: Ved beskrivelsen af begrundelsen for oprettelsen af en serviceaftale skal følgende oplysninger inkluderes:*
  - *Hvem skal have adgang?*
    Eksempel: Denne Serviceaftale skal bruges for at løsning X kan tilgå service Y for kommune Z.
  - *Hvad gives der adgang til?*
    *Eksempel: Serviceaftalen er oprettet i forbindelse med udviklingen af IT-system X, for at tillade adgang til data Y. Herunder skal det beskrives, hvordan de enkelte dataafgrænsninger afgrænser data, som kan tilgås. Der skal specifikt angives en årsag, hvis en valgfri dataafgrænsning fravælges eller indeholder en *-markering (uden effekt). Dette skal gøres i et forretningsmæssigt forståelsessprog.*
  - *Hvorfor gives der adgang?*
    Eksempel: Serviceaftalen anmodes i forbindelse med projekt X.

Da begrundelsen i en serviceaftale er det eneste sted, hvor en godkender er i stand til at få oplysninger omkring brugen og begrundelsen for en serviceaftale, er det vigtigt at være grundig i udfyldelsen af denne.

Vigtigt: Vær opmærksom på at retningslinjerne som beskrevet ovenfor skal overholdes, ellers vil en serviceaftale som udgangspunkt blive afvist.

Fortsæt til trin 2 - System ved at trykke på ”Næste”.

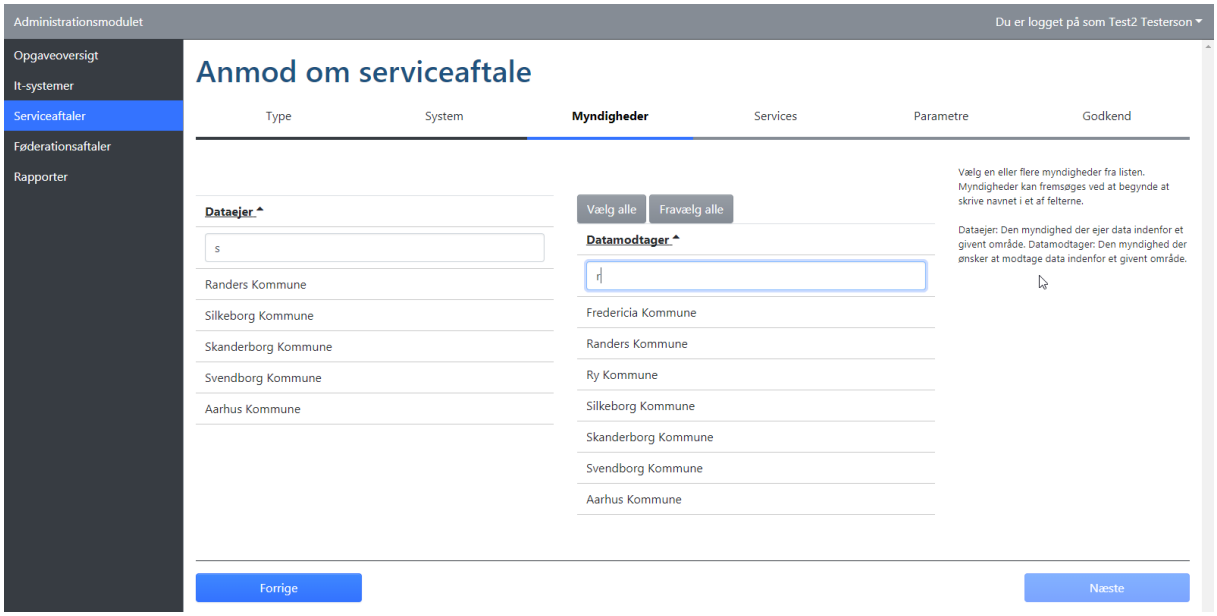
2. System



Under trin 2 - System - skal du vælge det anvendersystem som skal kalde de services, der indgår i aftalen. Du kan fremsøge et system i felterne på UUID, Navn og Leverandør. Vælge et system fra listen ved at klikke på den.

Fortsæt til trin 3 – Myndigheder ved at trykke på ”Næste”.

3. Myndigheder

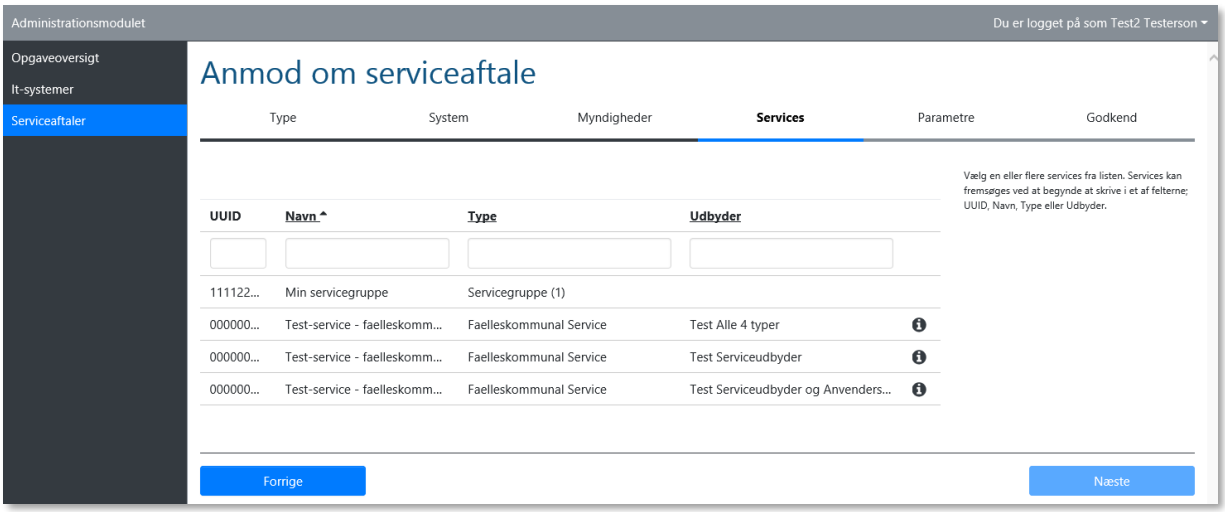


Under trin 3 – Myndigheder - skal du vælge én eller flere myndigheder hvis data, skal behandles af det anvendersystem, der indgår i serviceaftalen. Du kan fremsøge en myndighed via felterne Dataejer og Datamodtager. Vælg myndigheden ved at klikke på den fra listen.
Bemærk, at data ikke kan tilgås før myndigheden, har godkendt serviceaftalen.

Vær opmærksom på at skærmbilledet ovenfor viser en aftale af typen ”med videregivelse af data”, dette er den mest komplekse type af serviceaftale. Hvis en serviceaftale af typen ”uden videregivelse af data” er valgt, vil det kun være muligt at vælge hvilke myndigheder der er datamodtagere.

Fortsæt til trin 4 - Services ved at trykke på ”Næste”.

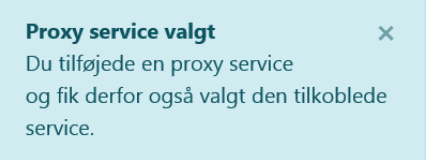
4. Services



Under trin 4 - Services - skal du vælge én eller flere services som anvendersystemet skal kunne tilgå. Du kan fremsøge en service ved at søge i felterne UUID, Navn, Type og Udbyder. Vælg serviceaftale ved at klikke på den fra listen.

Mange services er udstillede med flere typer af sikkerhedsmodeller. For yderligere information kan man trykke på i'et på den enkel service.

Bemærk: Flere af de udstillede services i Administrationsmodulet vil være koblede services, idet Serviceplatformen fungerer som proxy for mange kildesystemer. Hvis en koblet service vælges, bliver begge services tilføjet til serviceaftalen. Nedenstående systembesked vil blive vist hvis en koblet services vælges.



Bemærk: services af typen "Filservice med rutning" kan kun vælges hvis anvendersystemet har SSH opsat (SSH-brugernavn, SSH-nøgle samt e-mail).

Fortsæt til trin 5 - Parametre ved at trykke på "Næste".

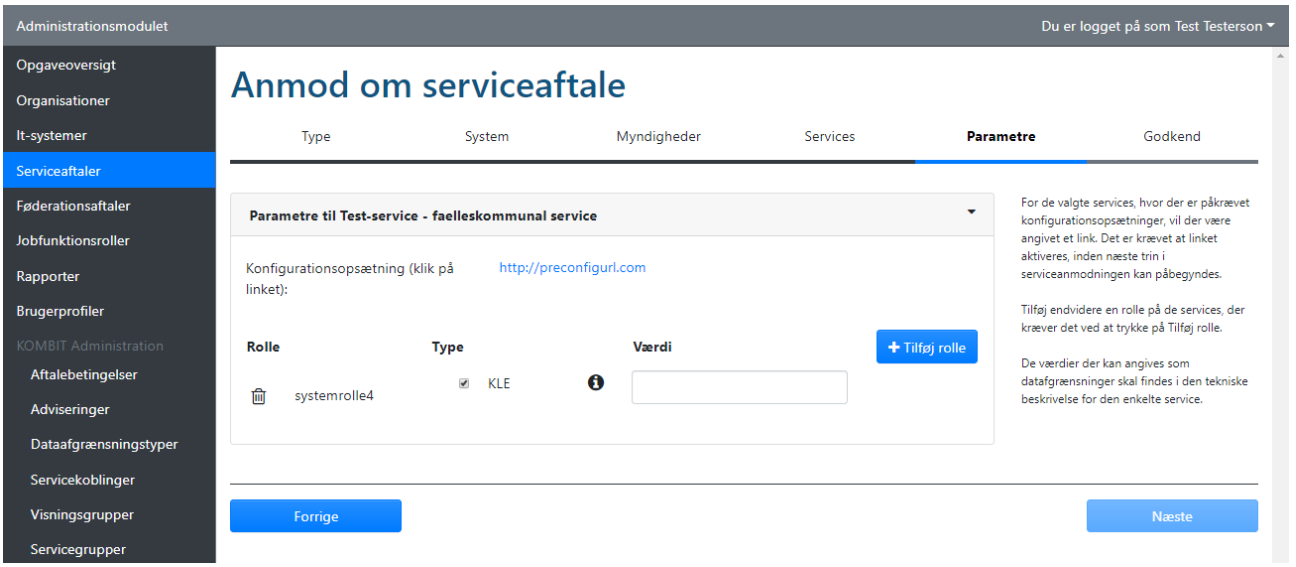
5. Parametre

Under trin 5 - Parametre - skal du tilføje serviceparametre, hvis det er påkrævet ud fra de services, du har valgt.

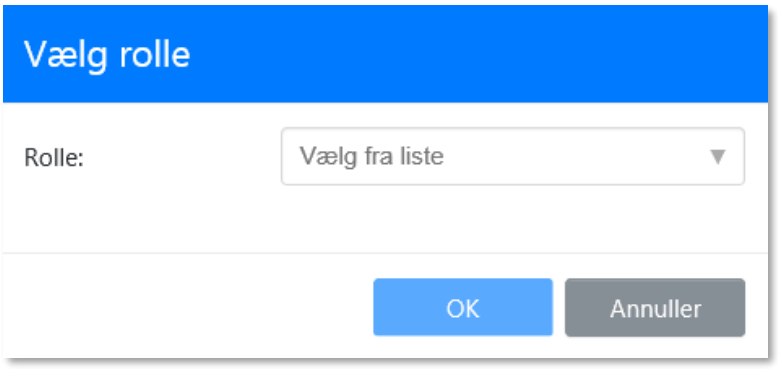
Generelt for alle services, er der påkrævet konfigurationsopsætninger, hvor man skal aktivere et link inden næste trin i serviceanmodningen kan påbegyndes.

Nedenstående services har yderligere serviceparametre som skal vælges.

- Fælles kommunal service:



For at tilføje rolle til en service, tryk på "Tilføj rolle". For mange services gælder, at de ikke skelner mellem forskellige roller. I så fald kan man kun vælge rollen "Dummy".



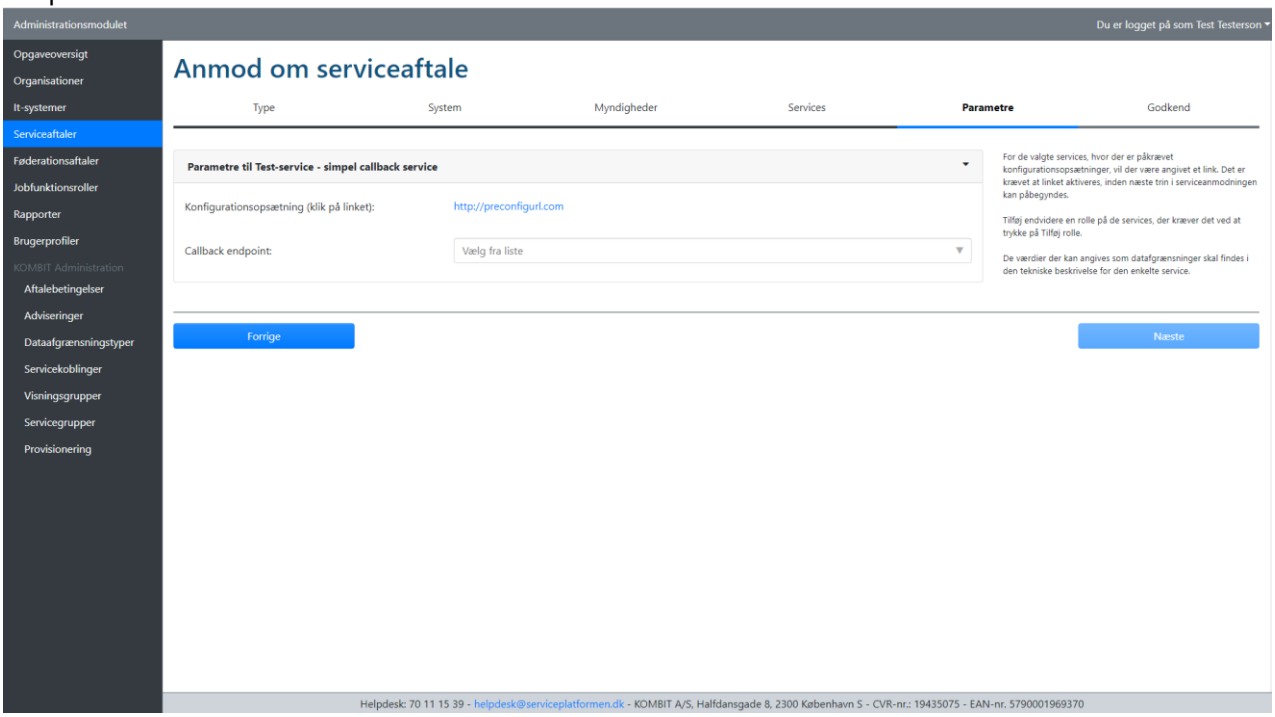
Hvis du ikke ønsker at angive specifikke dataafgrænsningstyper og værdier til rollen, kan du fjerne fluebenet i dataafgrænsningstypen.

De værdier der kan angives, skal findes i den tekniske beskrivelse for den enkelte service. For de services der pt. anvender de fælleskommunale dataafgrænsningstyper; KLE, Følsomhed, Organisatorisk Enhed og It-system kan du se de gyldige værdier her.

Beskrivelse af dataafgræsningstypen kan findes ved tryk på infoikonet.

Bemærk: Afgrænser du en dataafgrænsning med et wildcard (*), skal du angive årsagen hertil i begrundelsen for serviceaftalen (trin 1).

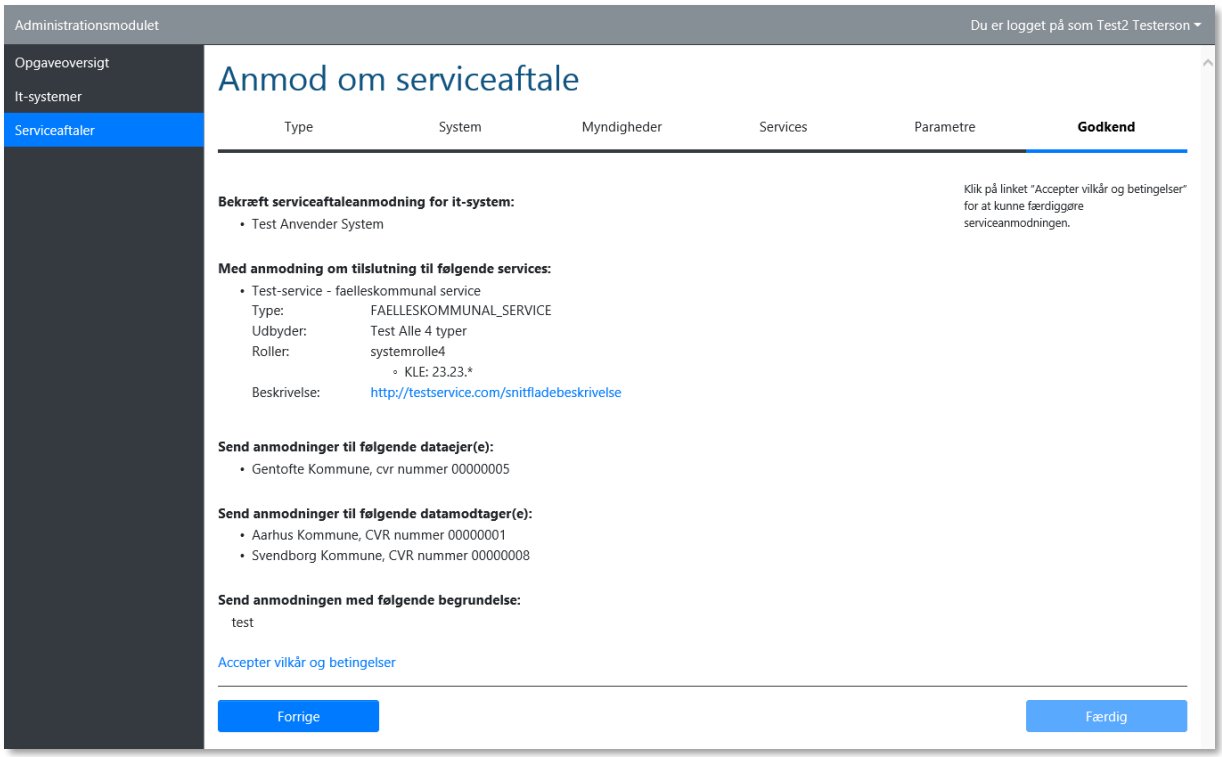
- Simpel callback service:



Da en callback service kun kan vælges, hvis anvendersystemet som indgår serviceaftalen, har et eller flere callback endpoints, skal man her specificere hvilket af disse endpoints man gerne vil have serviceaftalen skal knyttes til.

Fortsæt til trin 6 – Godkend ved at trykke på ”Næste”.

6. Godkend



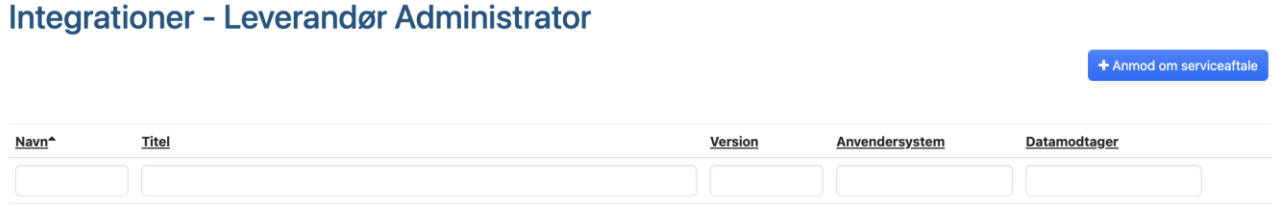
Under trin 6 - Godkend - skal du læse anmodningen igennem og klikke på linket ”Accepter vilkår og betingelser”. Læs vilkår og betingelserne og accepter dem for at kunne færdiggøre anmodningen. Afslut med at trykke på ”Færdig”.

Resultat: Anmodningen om serviceaftalen er sendt til godkendelse hos den/de valgte myndighed/myndigheder.

5.11.2 Anmodning ved brug af Integrationer

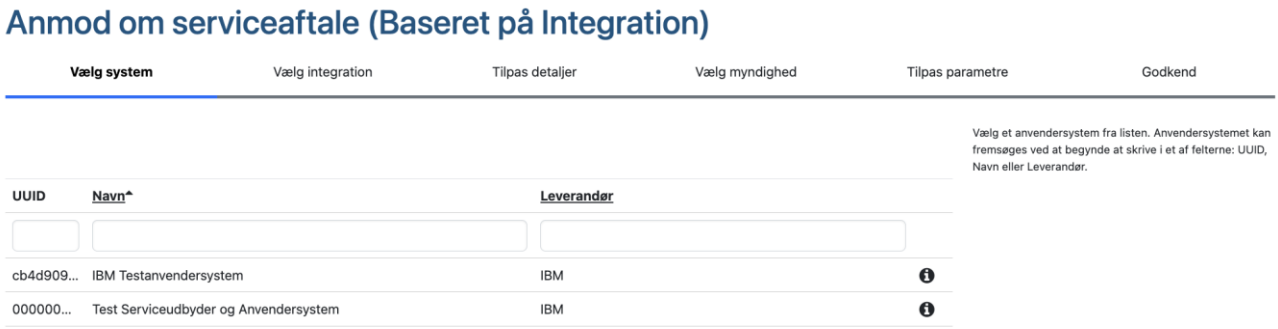
Vejledning:

I Administrationsmodulet skal du vælge punktet ”Integrationer for Leverandøradministrator” i venstremenuen. Herfra får du overblik over serviceaftaler, der allerede er anmodet om, organiseret efter Integrationsversioner.



For at anmode om en serviceaftale, skal du trykke på knappen ”Anmod om serviceaftale”. Herefter skal du igennem seks trin for at gennemføre anmodningen: Vælg system, Vælg integration, Tilpas detaljer, Vælg myndighed, Tilpas parametre og Godkend.

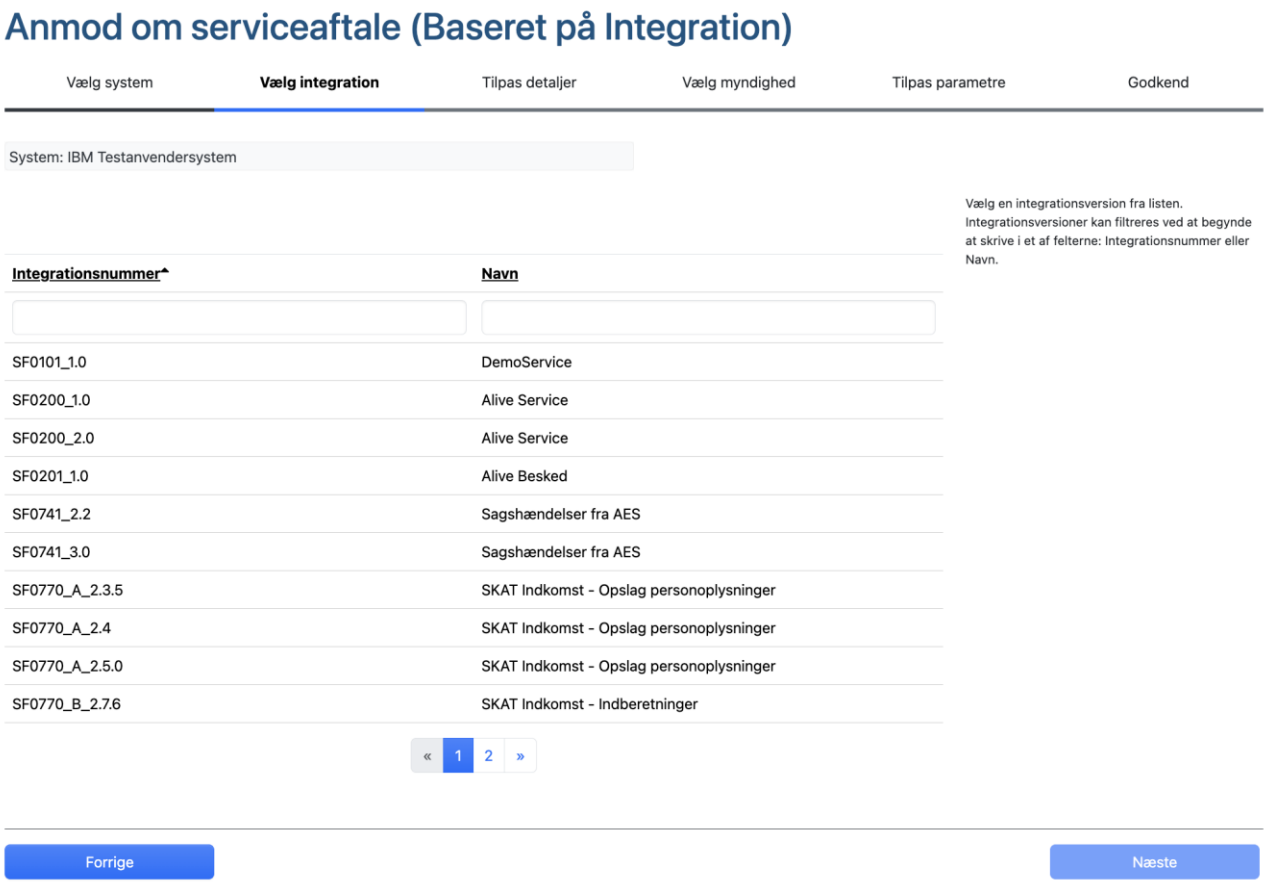
1. Vælg system



Under trin 1 – Vælg system – skal du vælge det anvendersystem som skal kalde de services, der indgår i aftalen. Du kan fremsøge et system i felterne på UUID, Navn og Leverandør. Vælg et system fra listen ved at klikke på det.

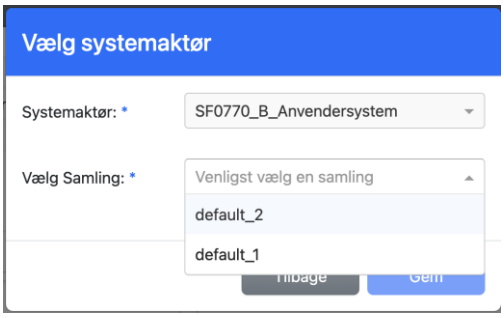
Fortsæt til trin 2 ”Vælg integration” ved at trykke på ”Næste”.

2. Vælg integration



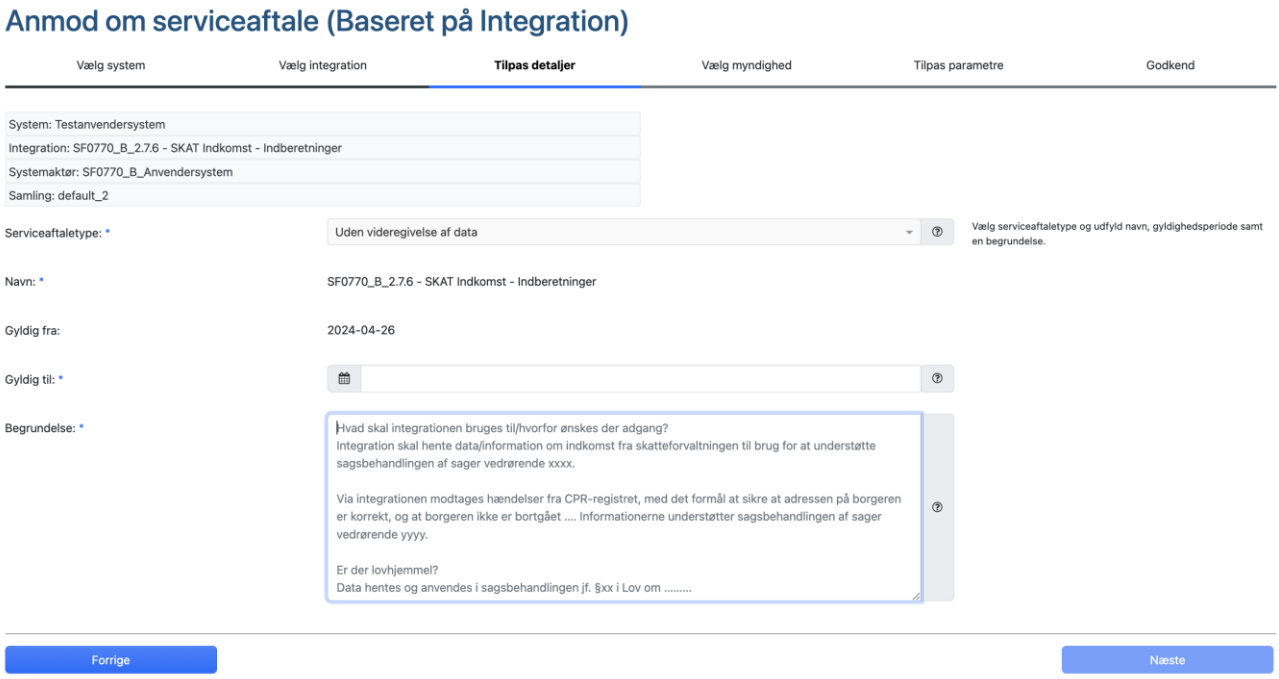
Under trin 2 – Vælg integration – skal du vælge et Integrationsnummer, som svarer til det anvendelsesscenarie, du anmoder om. Du kan fremsøge den ønskede integration ved at søge i felterne Integrationsnummer, Titel og Version. Vælg Integration ved at klikke på én fra listen.

Når du vælger en Integration, kan du i visse tilfælde blive mødt af dialogen nedenfor. Du vil blive bedt om at vælge en Systemaktør, hvis der for den pågældende Integration er flere Systemaktører tilknyttet. Systemaktøren vil sædvanligvis give et entydigt sortiment af Services, som rollen forventes at betjene sig af. Der kan dog for nogle få Systemaktører være tilknyttet flere samlinger af services, som hver især repræsenterer en variant, som Systemaktøren kan vælge at benytte. I så fald skal der også vælges hvilken samling, Systemaktøren skal benytte.



Fortsæt til trin 3 – Tilpas detaljer – ved at trykke på ”Næste”.

3. Tilpas Detaljer



Serviceaftaletype kan være en af nedenstående. Hvis alle Services i den service-samling, som følger med den valgte Systemaktør, understøtter videregivelse af data, vil brugeren skulle træffe valg om type. Ellers vil typen være forvalgt til ’Uden videregivelse af data’

- **Uden videregivelse af data (standardaftale):**
  Ved valg af denne aftaletype, betyder det, at du anmoder om én eller flere af myndigheders data

- **Med videregivelse af data, flere datamodtagere:**
  Ved valg af denne aftaletype, betyder det, at du på vegne af flere myndigheder tilgår én myndigheds data
- **Med videregivelse af data, flere dataejere:**
  Ved valg af denne aftaletype, betyder det, at du på vegne af én myndighed tilgår flere myndigheders data
- **Med videregivelse af data, én dataejer og én datamodtager:**
  Ved valg af denne aftaletype, betyder det, at du på vegne af én myndighed tilgår én anden myndigheds data

Gyldig til: Udfyld hvornår aftalen skal være gyldig til.

> ***Retningslinjer for eksternt testmiljø****: Som udgangspunkt bør gyldighedsperioden for en serviceaftale være højst 1 år. Hvis en serviceaftale ikke har en gyldighedsperiode, bliver denne sat til 3 måneder i forbindelse med godkendelse med mindre andet er aftalt.*
> ***Retningslinjer for produktionsmiljøet****: Gyldighedsperioden ved oprettelse af en serviceaftale skal aftales mellem leverandør og myndighed i forbindelse med at det relevante IT-systems produktionssættes.*

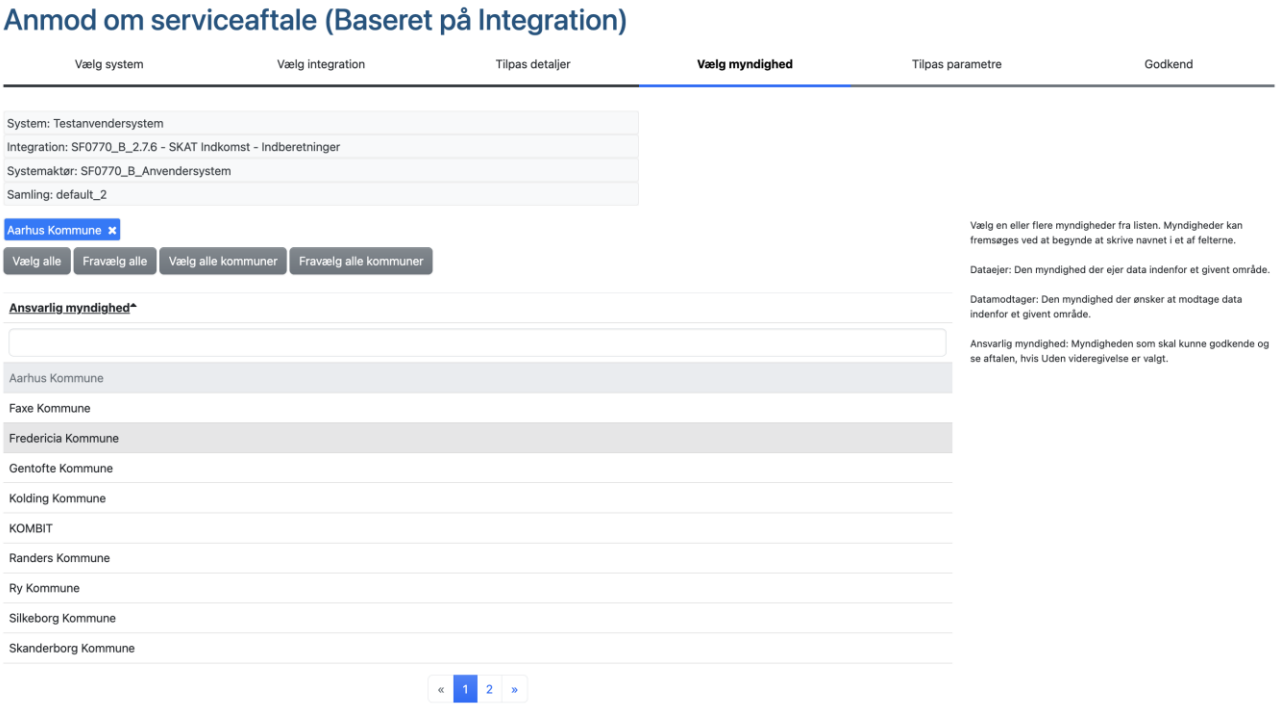
Begrundelse: Tilføj begrundelse for anmodningen om serviceaftalen. Begrundelsen ses når myndigheden skal godkende anmodningen.

> ***Retningslinjer****: Ved beskrivelsen af begrundelsen for oprettelsen af en serviceaftale skal følgende oplysninger inkluderes:*
>
> - *Hvem skal have adgang?*
>   *Eksempel: Denne Serviceaftale skal bruges for at løsning X kan tilgå service Y for kommune Z.*
> - *Hvad gives der adgang til?*
>   *Eksempel: Serviceaftalen er oprettet i forbindelse med udviklingen af IT-system X, for at tillade adgang til data Y. Herunder skal det beskrives, hvordan de enkelte dataafgrænsninger afgrænser data, som kan tilgås. Der skal specifikt angives en årsag, hvis en valgfri dataafgrænsning fravælges eller indeholder en *-markering (uden effekt). Dette skal gøres i et forretningsmæssigt forståelsessprog.*
> - *Hvorfor gives der adgang?*
>   *Eksempel: Serviceaftalen anmodes i forbindelse med projekt X.*
>
> *Da begrundelsen i en serviceaftale er det eneste sted, hvor en godkender er i stand til at få oplysninger omkring brugen og begrundelsen for en serviceaftale, er det vigtigt at være grundig i udfyldelsen af denne***.**

Vigtigt: Vær opmærksom på at retningslinjerne som beskrevet ovenfor skal overholdes, ellers vil en serviceaftale som udgangspunkt blive afvist.

Fortsæt til trin 4 – Vælg myndighed – ved at trykke på ”Næste”.

4. Vælg myndighed

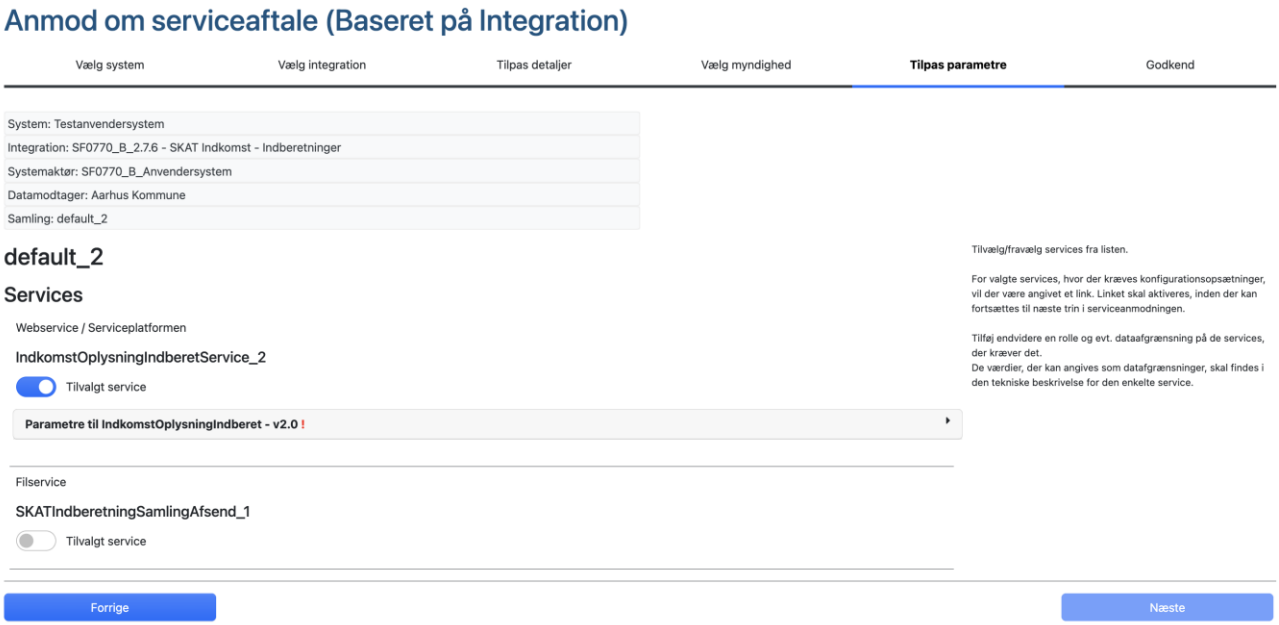


Under trin 4 – Vælg myndighed - skal du vælge én eller flere myndigheder hvis data, skal behandles af det anvendersystem, der indgår i serviceaftalen. Du kan fremsøge en myndighed via felterne Dataejer og Datamodtager. Vælg myndigheden ved at klikke på den fra listen. Bemærk, at data ikke kan tilgås før myndigheden, har godkendt serviceaftalen.

Vær opmærksom på at skærmbilledet ovenfor viser en aftale af typen ”Uden videregivelse af data”. Hvis typen indebærer videregivelse af data, skal der vælges både afgivende og modtagende myndighed(er)

Fortsæt til trin 5 – Tilpas parametre – ved at trykke på ”Næste”.

5. Tilpas parametre



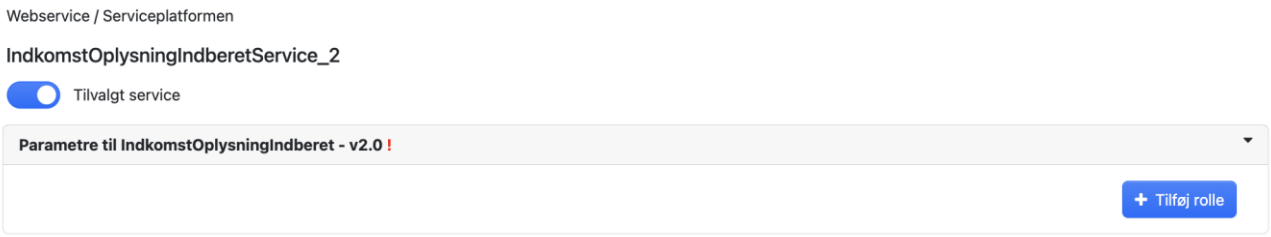
Under trin 5 – Tilpas parametre - skal du til-/fravælge services og tilføje serviceparametre, hvis det er påkrævet for de services, du har valgt.

Den i trin 2 valgte Systemaktør (og evt. samling) vil definere de services, der kan vælges. Visse services er obligatoriske og er derfor forvalgt.

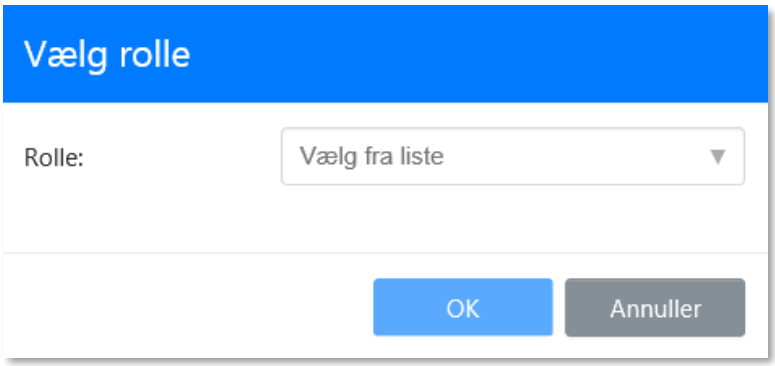
For visse services er der påkrævet konfigurationsopsætninger, hvor man skal aktivere et link, inden man kan springe videre til næste trin i serviceaftaleanmodningen.

For visse services vil der være yderligere serviceparametre, som skal vælges.

- Fælles kommunal service:



For at tilføje rolle til en service, tryk på ”Tilføj rolle”. For mange services gælder, at de ikke skelner mellem forskellige roller. I så fald kan man kun vælge rollen ”Dummy”.

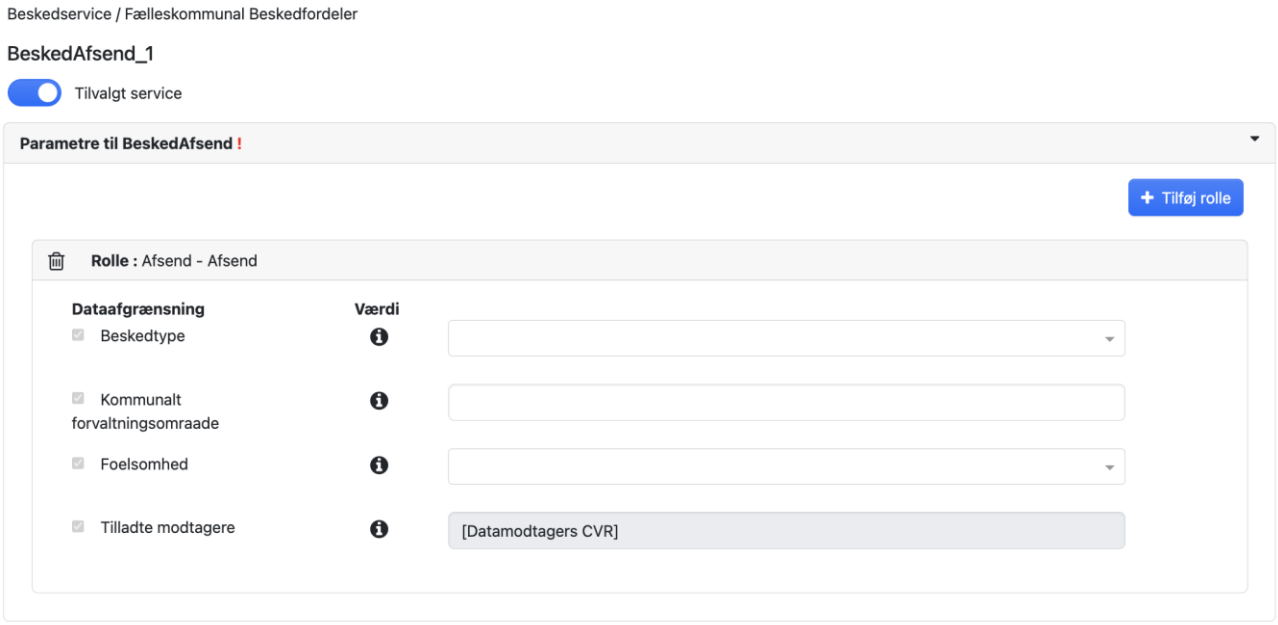


Hvis du ikke ønsker at angive specifikke dataafgrænsningstyper og værdier til rollen, kan du fjerne fluebenet i dataafgrænsningstypen, med mindre typen er påkrævet. Beskrivelse af dataafgræsningstypen kan findes ved tryk på infoikonet.

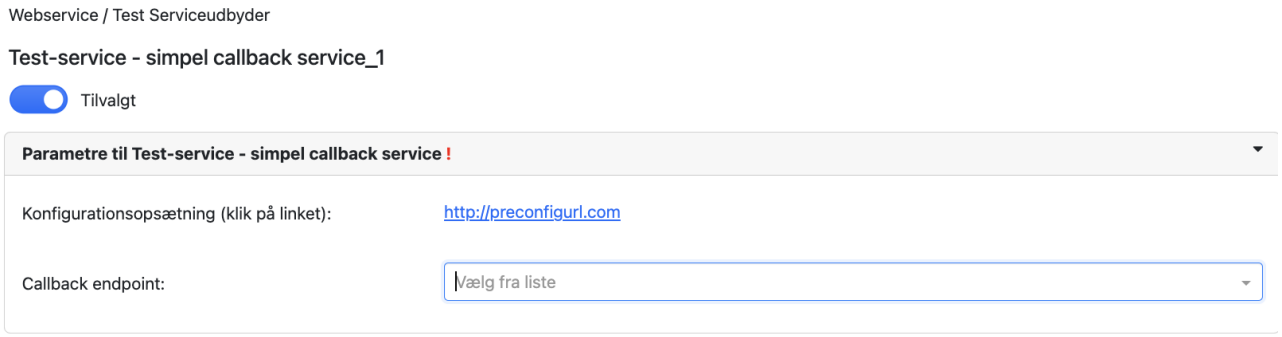
Visse dataafgrænsningstyper har et fast udfaldsrum, der kan vælges blandt. For andre skal værdien angives ved indtastning. De værdier der kan angives, skal findes i den tekniske beskrivelse for den enkelte service. For de services der pt. anvender de fælleskommunale dataafgrænsningstyper; KLE, Følsomhed, Organisatorisk Enhed og It-system kan du se de gyldige værdier her.

Dataafgrænsningsværdien kan i visse tilfælde være givet gennem valget af Systemaktør. I så fald skal du ikke foretage nogen ændringer. Værdien kan også blive beregnet automatisk af systemet:

- Hvis værdien er forudfyldt med [IT-systemets UUID], indsætter systemet automatisk UUID for det Anvendersystem, som aftalen gælder for.
- Hvis værdien er forudfyldt med [Datamodtagers CVR], indsætter systemet automatisk CVR-nummeret for datamodtageren. Hvis der er valgt flere datamodtagere, etableres individuelle serviceaftaler for hver datamodtager med datamodtagerens CVR-nummer som dataafgrænsningsværdi.



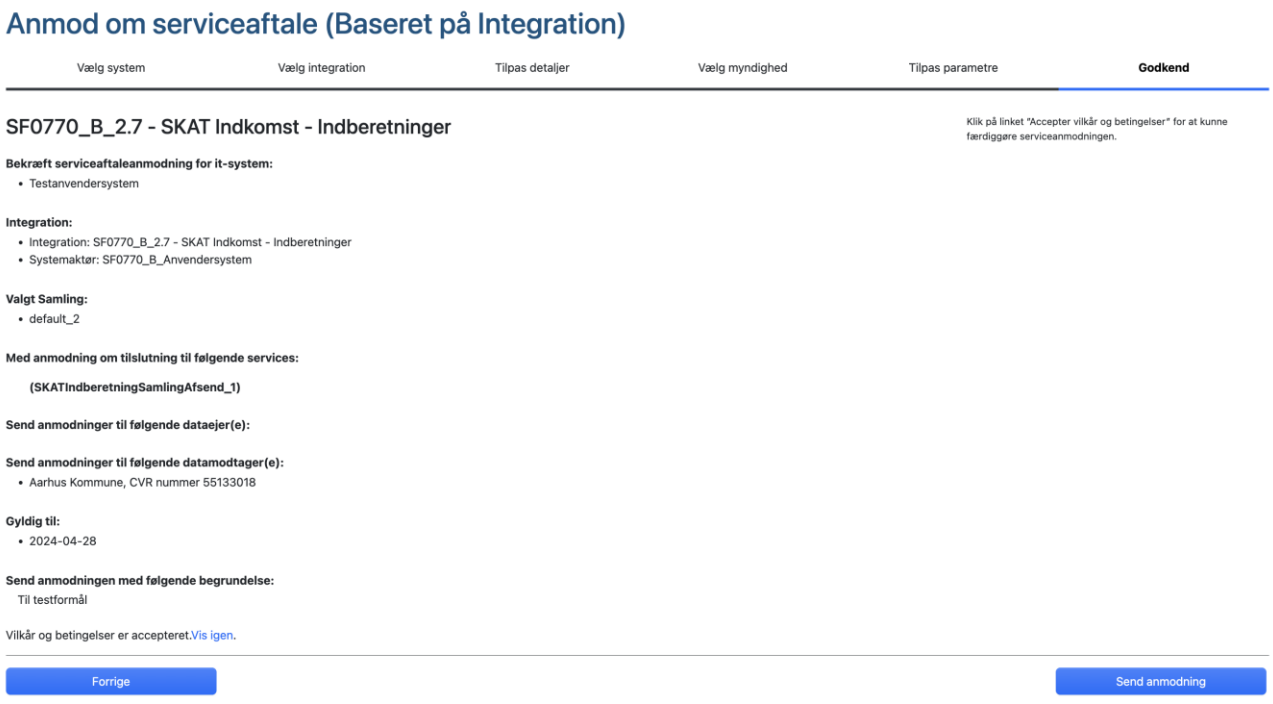
- Simpel callback service:



Da en callback service kun kan vælges, hvis anvendersystemet som indgår serviceaftalen, har et eller flere callback endpoints, skal man her specificere hvilket af disse endpoints man gerne vil have, at serviceaftalen skal knyttes til.

Fortsæt til trin 6 – Godkend – ved at trykke på ”Næste”.

6. Godkend



Under trin 6 - Godkend - skal du læse anmodningen igennem og klikke på linket ”Accepter vilkår og betingelser”. Læs vilkår og betingelserne og accepter dem for at kunne færdiggøre anmodningen. Afslut med at trykke på ”Færdig”.

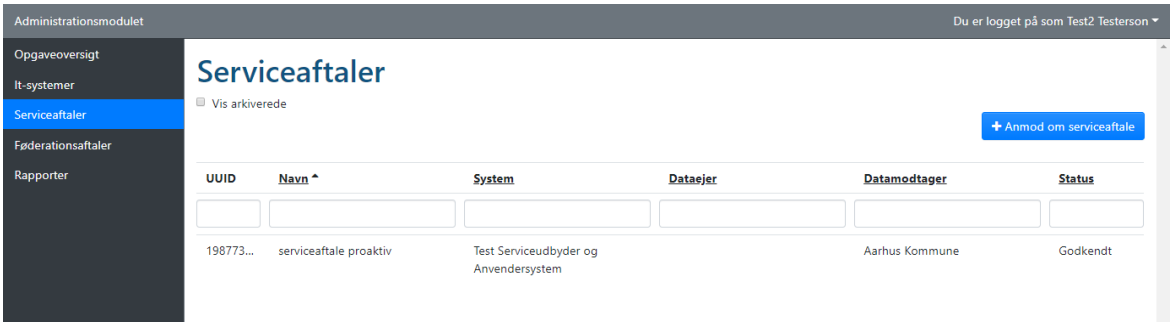
Resultat: Anmodningen om serviceaftalen er sendt til godkendelse hos den/de valgte myndighed/myndigheder.

5.12 Vis serviceaftaler

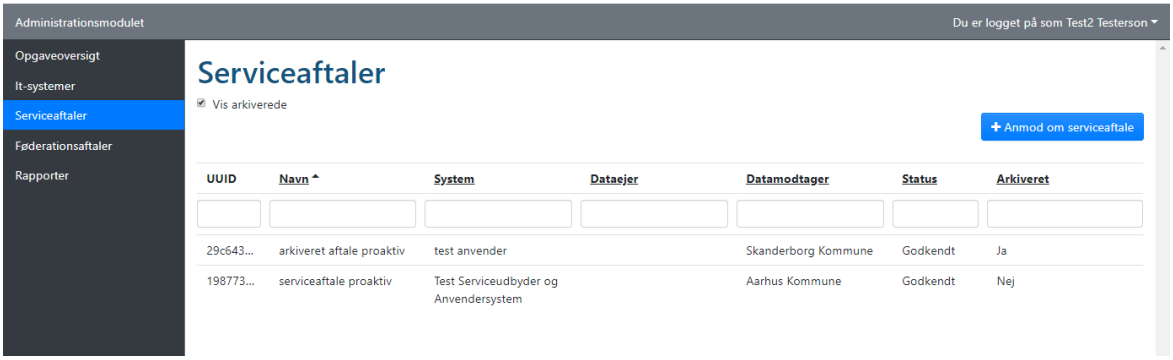
Brugeren: Med rollen Leverandøradministrator kan du få vist de serviceaftaler, som din organisation har anmodet om, både aktive og arkiverede.

Vejledning:

1. I Administrationsmodulet skal du vælge punktet Serviceaftaler i venstremenuen. Herefter får du et overblik over serviceaftaler tilknyttet din organisation. Serviceaftalerne kan have status ”Afventer”, ”Godkendt”, ”Afvist” eller ”Delvis godkendt”. ”Delvis godkendt” betyder at aftalen afventer behandling fra en af de omfattede myndigheder. Du kan fremsøge en serviceaftale ved at søge i felterne UUID, Navn, System, Dataejer, Datamodtager eller Status. Vælg en serviceaftale fra listen ved at klikke på den.

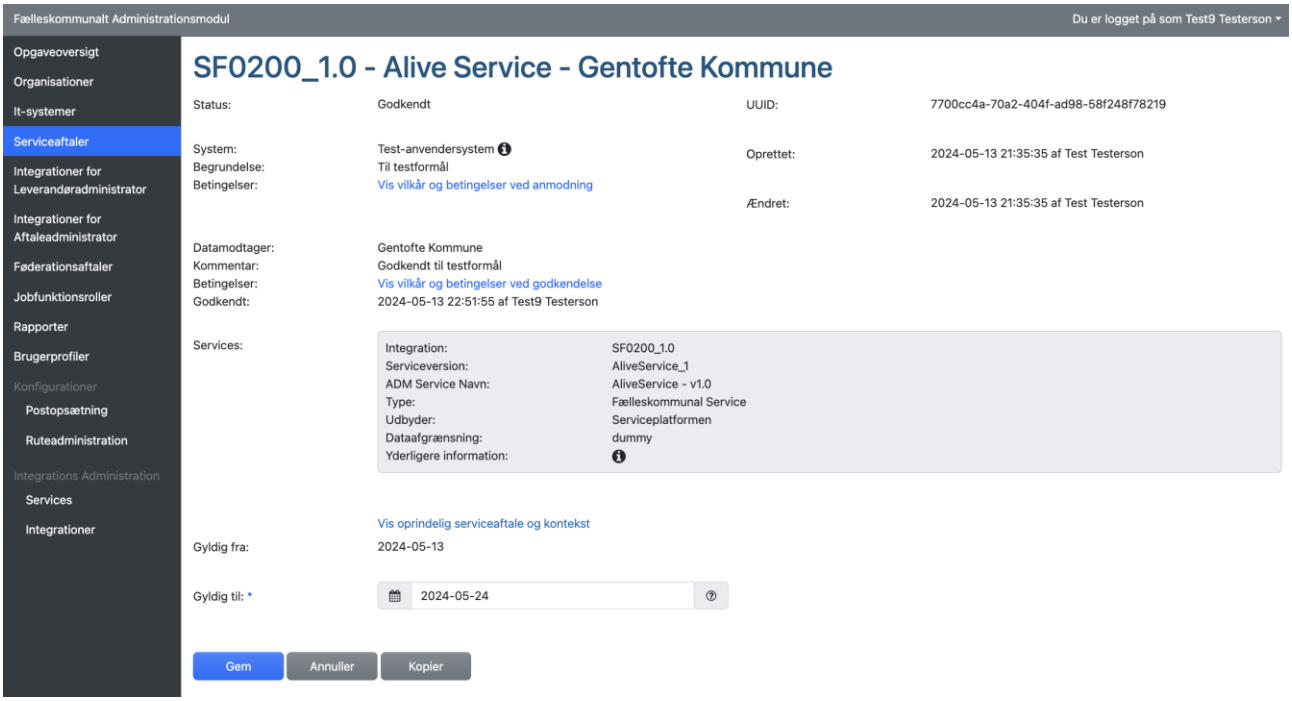


2. Ved tryk på ”Vis arkiverede” tilføjes en kolonne ”Arkiveret” til listen, og listen vil herefter indeholde både de aktive og de arkiverede serviceaftaler. Nu vil serviceaftaler med status ”Udløbet” også fremgå af listen, da disse arkiveres ved udløb.



Bemærk. Foruden normalt klik kan Ctrl+klik åbne aftalen i en ny tab og Shift+klik i et nyt browservindue.

3. Når du har valgt en ikke arkiveret aftale, kan du se de detaljer, som er tilknyttet aftalen.

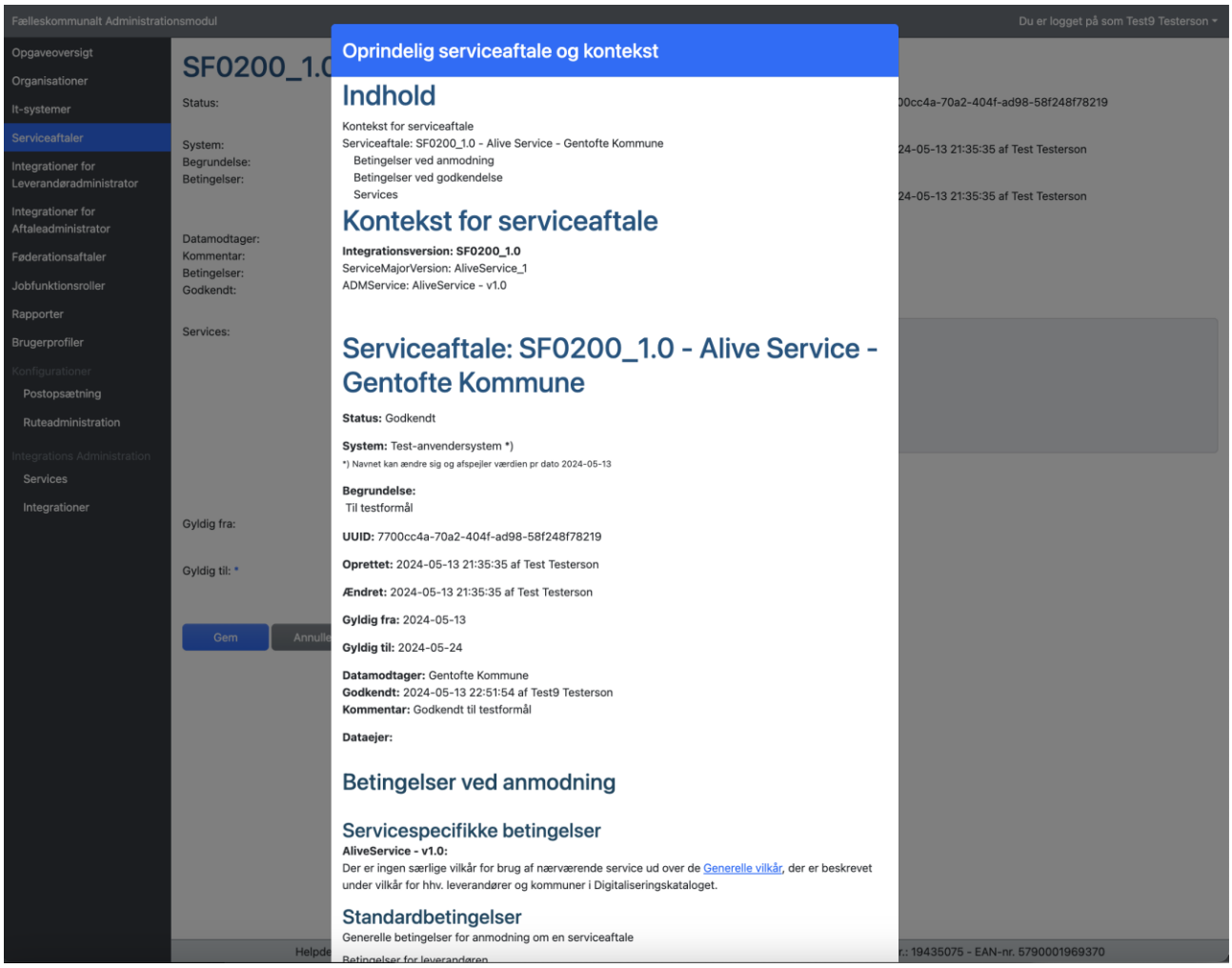


Det er kun muligt at redigere ”Gyldig til” datoen. Hvis der allerede står en dato i feltet, kan den kun ændres til en tidligere dato, dog tidligst dagen efter dags dato. Når datoen for ”Gyldig til” er overskredet, er serviceaftalen ikke længere aktiv.

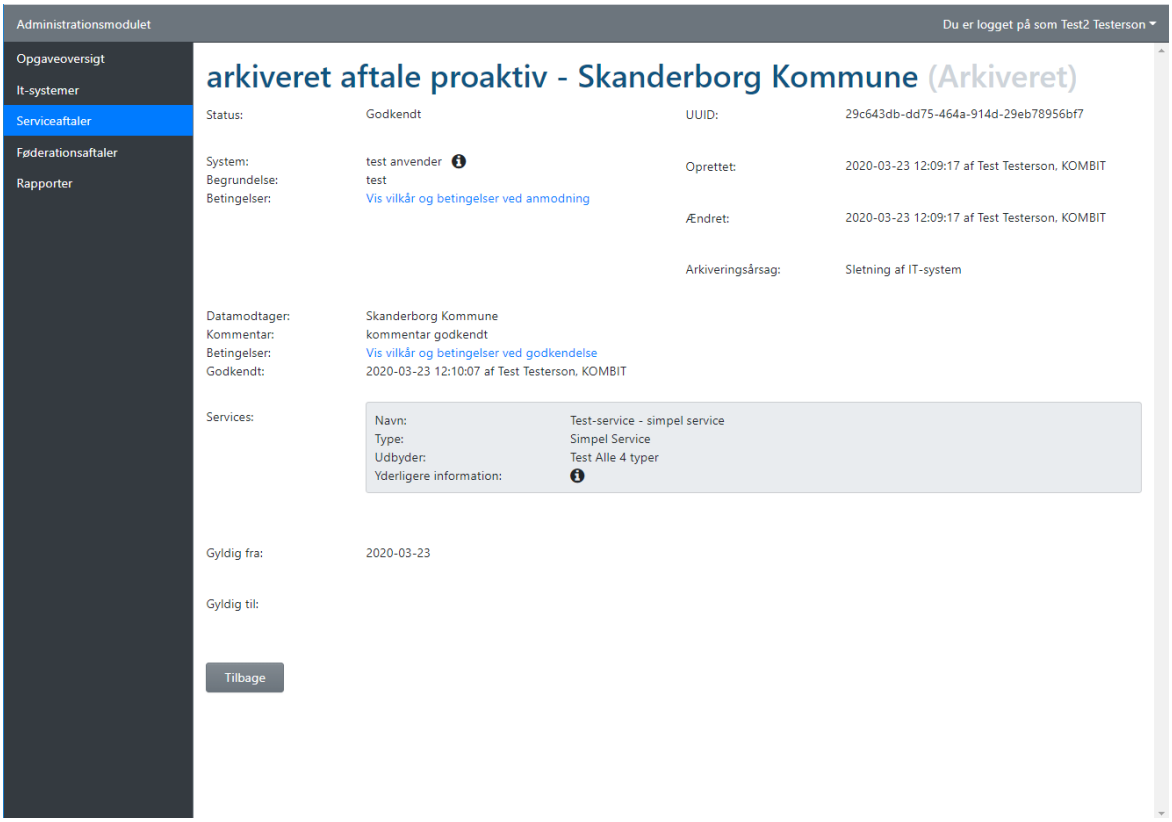
- Status: Her vises status for serviceaftalen
- System: Her vises fra hvilket system, anmodningen om serviceaftalen kommer fra
- Begrundelse: Her vises it-leverandørens begrundelse for anmodningen om serviceaftalen
- Betingelser (under system): Her vises vilkår og betingelser som it-leverandøren har godkendt i forbindelse med anmodningen
- Datamodtager/Dataejer: Den myndighed der har godkendt/afvist aftalen
- Kommentar: Myndighedens kommentar ved godkendelse/afvigelse af aftalen
- Betingelser (under kommentar): Her vises vilkår og betingelser som myndigheden har godkendt i forbindelse med anmodningen
- Services: Her vises hvilke services der indgår i serviceaftalen. Hvis serviceaftalen er baseret på en Integration, vises desuden Integrationens navn og navnet på Servicen som den optræder i Integrationen.

4. Linket ”Vis oprindelig serviceaftale og kontekst” vises for godkendte serviceaftaler. Ved aktivering af linket åbner et vindue, hvor man kan se serviceaftalens oprindelige indhold og kontekst. Informationerne i dette vindue svarer for hovedpartens vedkommende til informationerne på siden, der linkes fra, men er struktureret som et samlet dokument.
En serviceaftale ændrer ikke aftalemæssigt indhold, efter den er indgået, men supplerende elementer med information om serviceaftalens sammenhæng kan ændre sig over tid, f.eks. navne på organisation, integration eller services. ”Vis oprindelig serviceaftale og kontekst” viser som hovedregel indholdet, som det fremstod på godkendelsestidspunktet for serviceaftalen. For ældre, aktive serviceaftaler, er det dog ikke nødvendigvis de oprindelige navne, der vises. I så fald vil det fremgå af visningen, hvornår oplysningerne er indsamlet. Med ”kontekst” refereres til informationer om den Integration, der har dannet grundlag for serviceaftalen. Disse oplysninger fremgår også.

Ældre serviceaftaler er blevet indgået, før indførelse af praksis med at registrere kontekster for aftalen. For disse kan der være udført en efterfølgende tilpasning fra KOMBITs side, så konteksten beskriver en eller flere Integrationer, hvis karakteristika svarer til indholdet af serviceaftalen.



5. Når du har valgt en arkiveret aftale, kan du se de detaljer, som er tilknyttet aftalen, intet kan redigeres, felterne er de samme felter som for en ikke arkiveret serviceaftale.



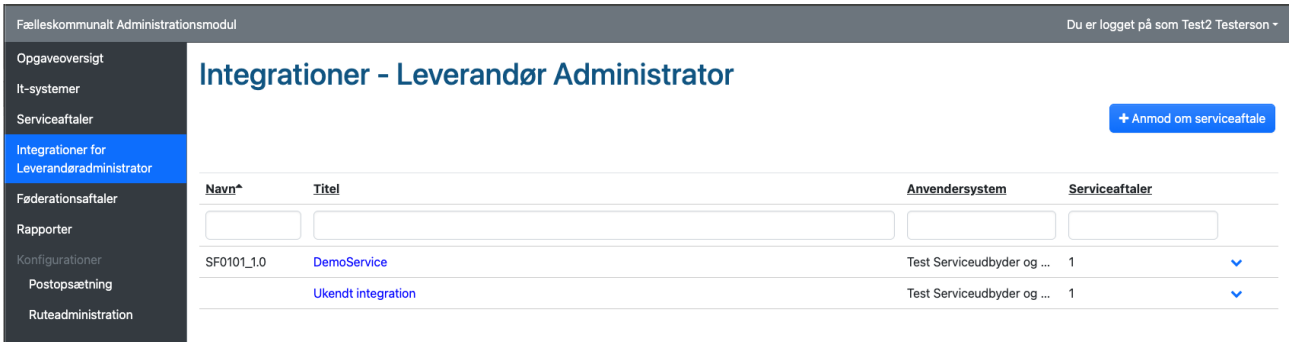
Resultat: Du har nu fået vist de serviceaftaler, der er tilknyttet din organisation.

5.13 Vis integrationer

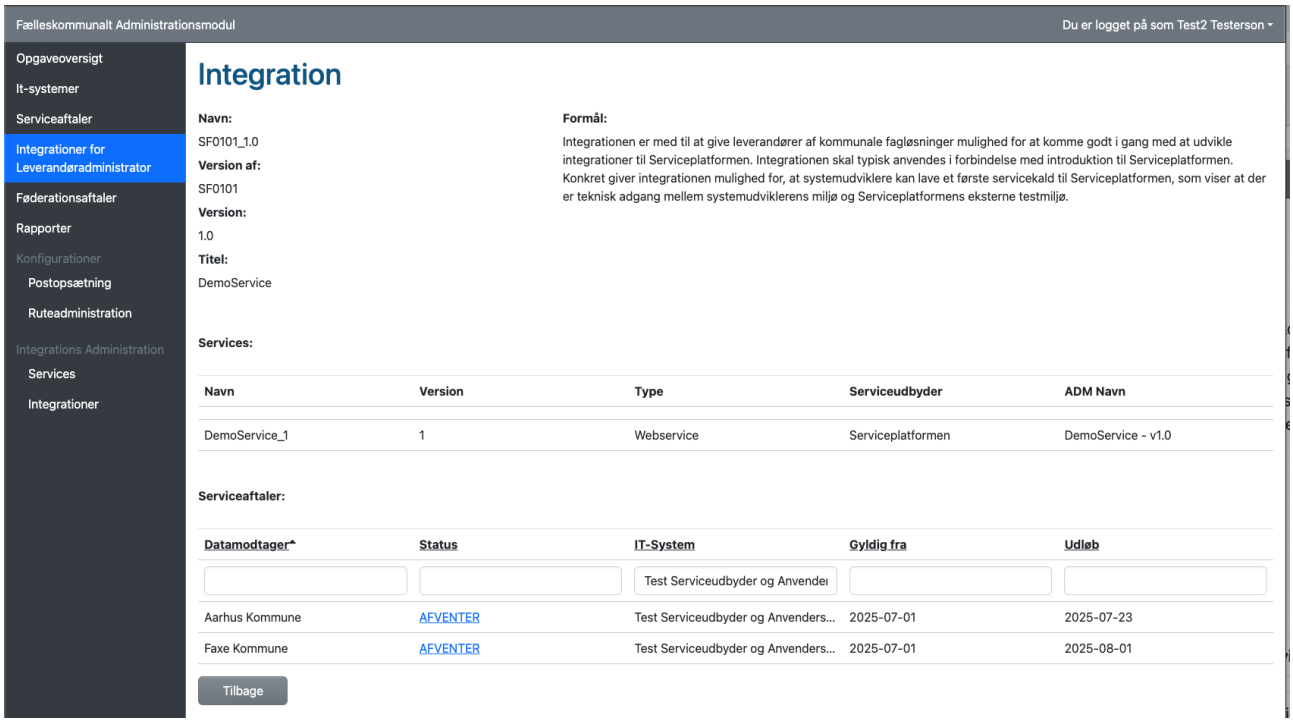
Brugeren: Med rollen Leverandøradministrator kan du få vist de serviceaftaler, som din organisation har anmodet om, organiseret efter Integrationer. Dette er et alternativ til fremgangsmåden beskrevet i afsnit 5.12.

Vejledning:

I Administrationsmodulet vælger du 'Integrationer for Leverandøradministrator'. Du får i første omgang vist en liste over Integrationsversioner og IT-Systemer (Anvendersystemer), der matcher med de serviceaftaler, din organisation her anmodet om:



Når du klikker i Titel-kolonnen i en række svarende til en specifik version af en Integration og et IT-System, kommer du til en side, der dels viser listen af services i Integrationen og dels viser din organisations serviceaftaler knyttet til denne kombination:



Herfra kan du klikke i Status-kolonnen for en konkret serviceaftale, hvorved du får vist serviceaftalen (Se afsnit 5.12)

5.14 Serviceaftaleoverblik (beta)

Menupunktet Serviceaftaleoverblik (beta) giver adgang til at navigere i serviceaftaler ud fra forskellige kriterier, der varierer med brugerens organisatoriske tilhørsforhold og rolle.

Brugeren: Med rollen Leverandøradministrator kan du få vist de serviceaftaler, som din organisations systemer indgår i, enten som anvendersystem eller som serviceudbyder. Serviceaftalerne kan være filtreret efter valg af It-system og/eller Integration, eller vises som en ufiltreret liste. Dette er et alternativ til fremgangsmåderne beskrevet i afsnit 5.12 og afsnit **Error! Reference source not found.**.

Vejledning:

I Administrationsmodulet vælger du 'Serviceaftaleoverblik (beta)'. Du får øverst vist to faneblade: Anvender og Udbyder.

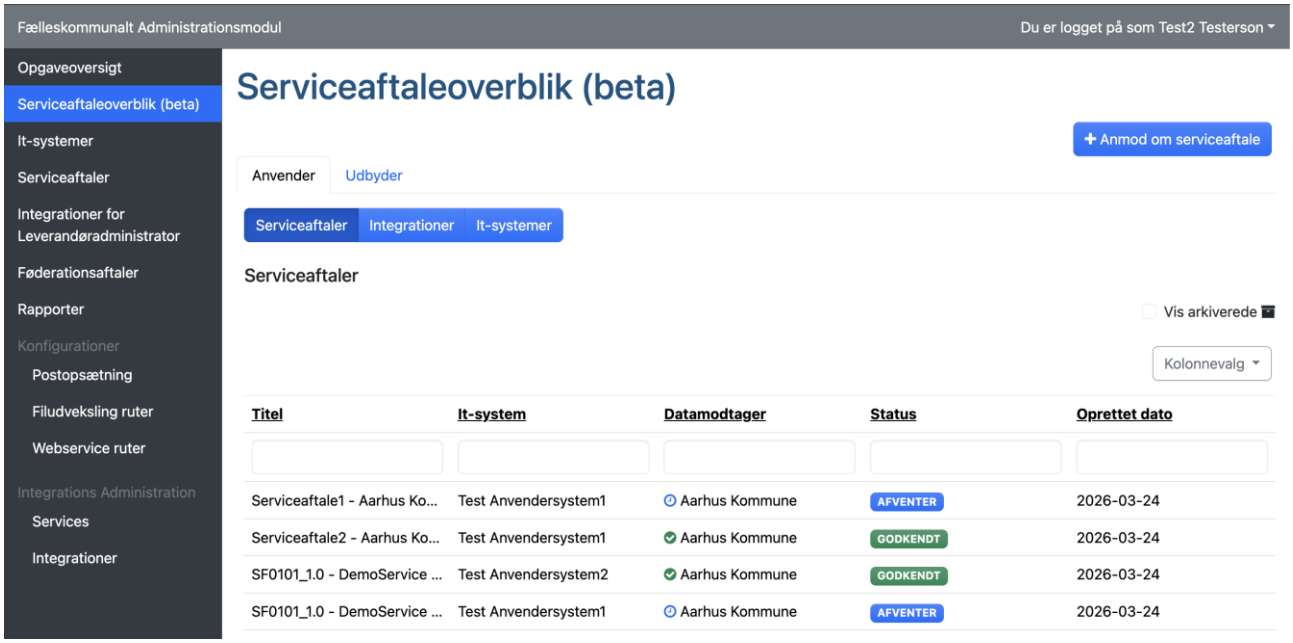
Under Anvender-fanen får du vist 3 under-faner: Serviceaftaler, Integrationer og It-systemer. Fanen Serviceaftaler er forvalgt.

Under Udbyder-fanen er der blot én under-fane, Services. Denne er forvalgt.

Her følger en beskrivelse af, hvordan de forskellige valg af faner for rollen Leverandøradministrator kan benyttes:

Anvender > Serviceaftaler:

Denne indgang giver en ufiltreret liste over alle de serviceaftaler, for hvilke brugerens organisation er leverandør af det benyttede anvendersystem. Listen indeholder i udgangspunktet serviceaftaler i status Godkendt, Afventer, Delvist godkendt eller Afvist. Ved markering af "Vis arkiverede" medtages også arkiverede serviceaftaler i listen, idet de fremstår med den status, de havde på arkiveringstidspunktet.

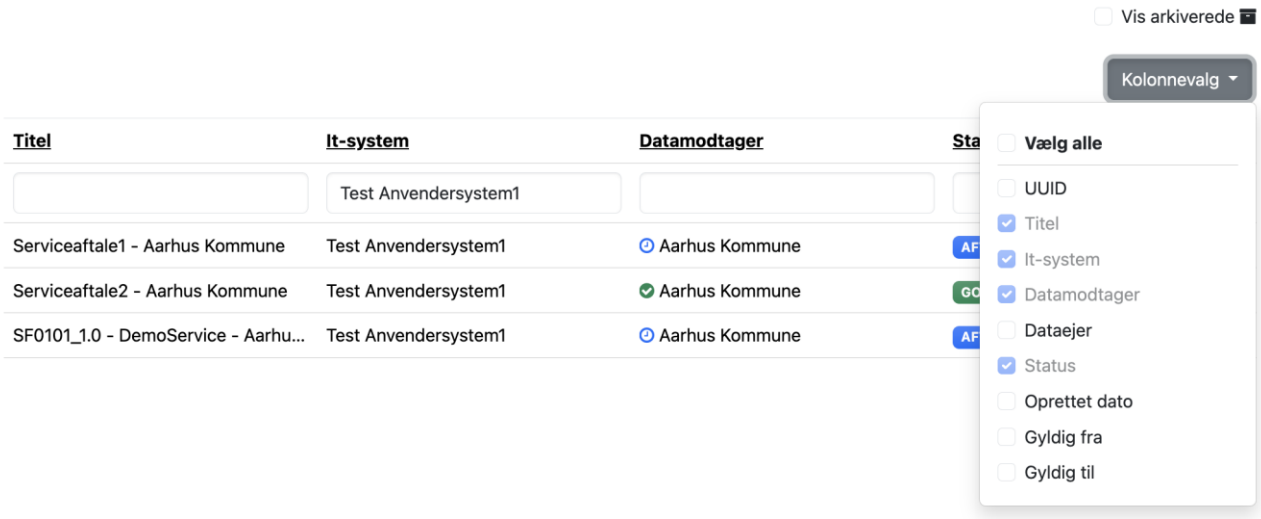


Fra denne liste kan man vælge en specifik serviceaftale, som vises som beskrevet i afsnit 5.12.

På Serviceaftaler-fanebladet er det muligt at vælge, hvilke kolonner, der skal vises ved klik på knappen Kolonnevalg. Kolonnerne Dataejer, Gyldig fra og Gyldig til kan tilvælges, mens Oprettet dato kan fravælges.

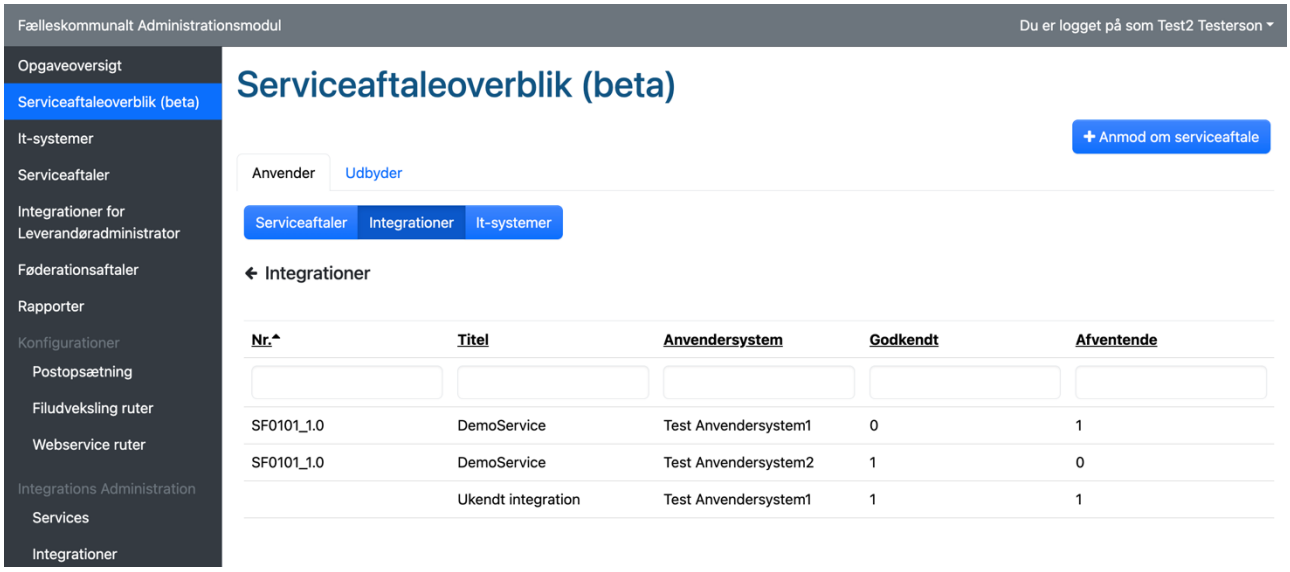
Det er også muligt at filterere på samtlige kolonner som vist for It-system-kolonnen nedenfor.

Filtreringskriterier og valg af kolonner på denne side huskes af systemet, også hvis du lukker din browser ned og starter op igen på et senere tidspunkt i samme browser.



Anvender > Integrationer:

Denne indgang giver en liste over alle de Integrationsversioner, som er knyttet til serviceaftaler i status Godkendt, Afventer eller Delvist godkendt, for hvilke anvendersystemet er leveret af brugerens organisation.



Kolonnerne Godkendt og Afventende viser, hvor mange serviceaftaler, der er i hhv. status Godkendt eller i en afventende status (dvs. Afventer eller Delvist Godkendt) for den pågældende kombination af Integrationsversion og Anvendersystem.

Når et element i listen aktiveres, fremkommer en side med en liste over de serviceaftaler, som opfylder ovenstående kriterier og er knyttet til den valgte kombination af Integrationsversion og Anvendersystem.

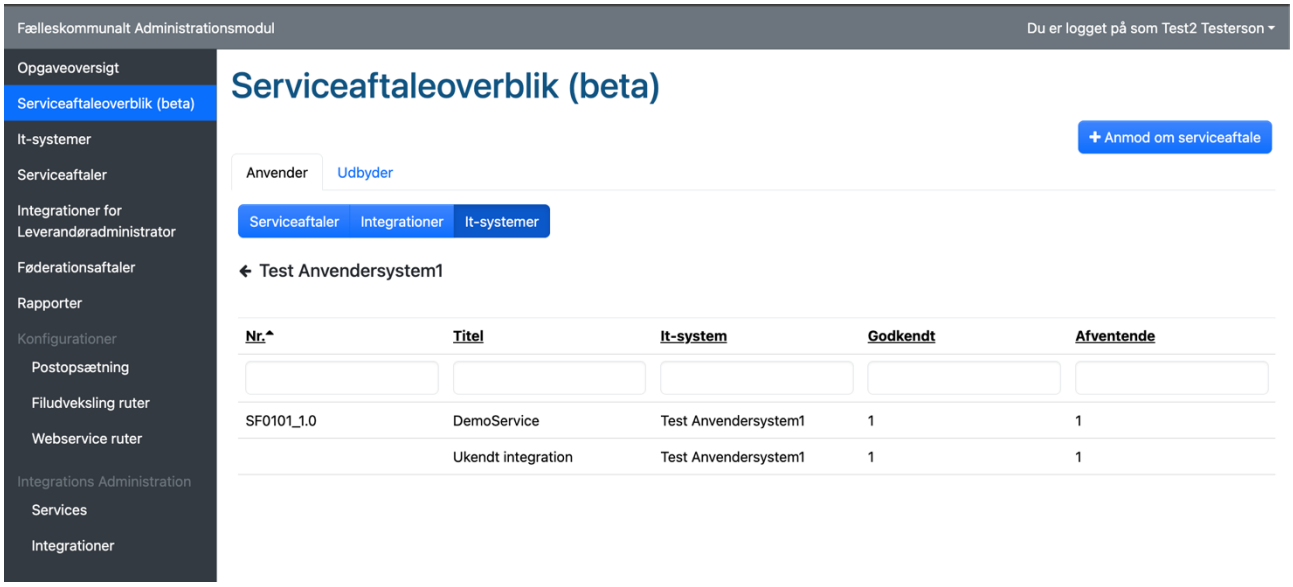
Virkemåden er i øvrigt som beskrevet under Anvender > It-systemer nedenfor.

Anvender > It-systemer:

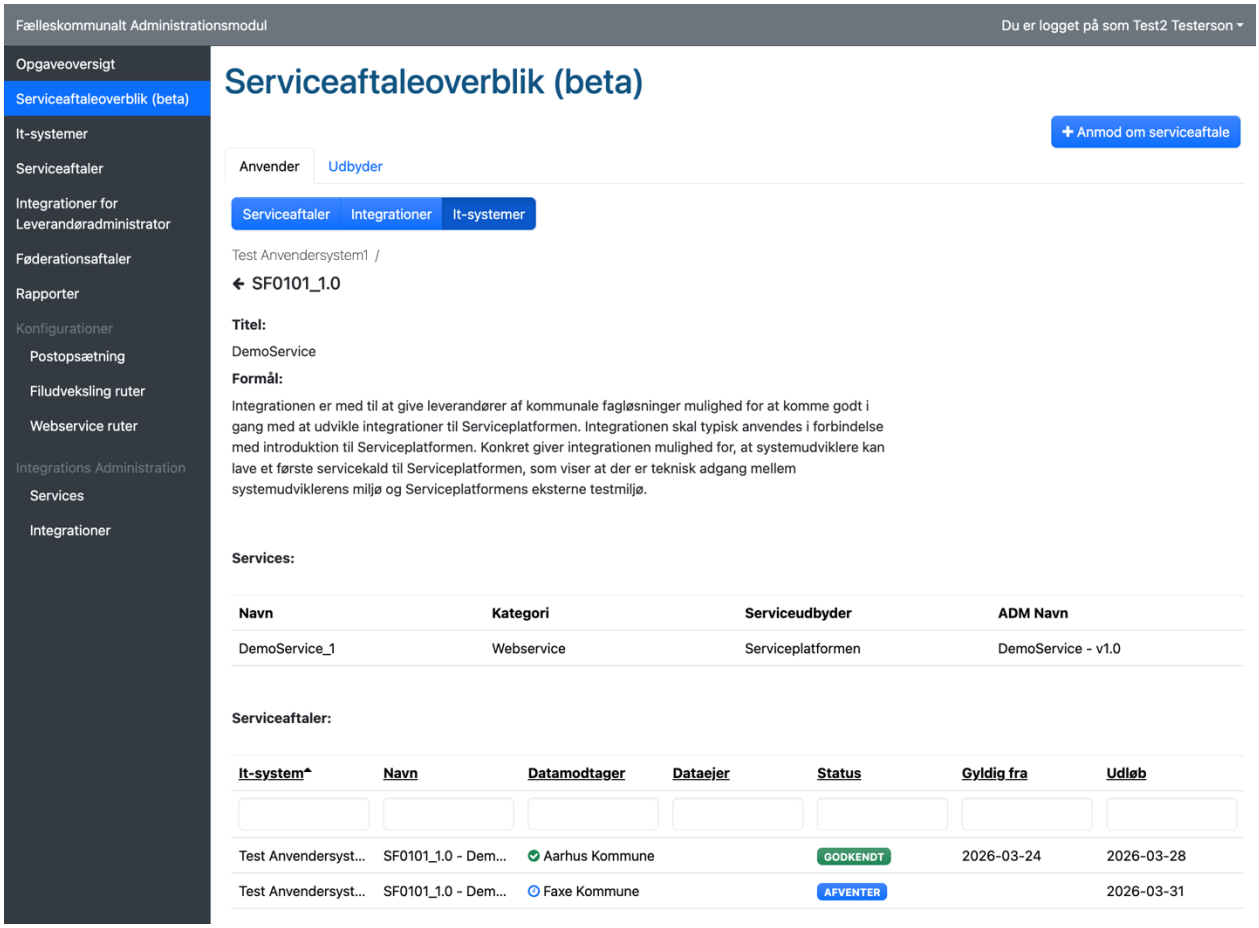
Denne indgang giver en liste over alle de It-systemer, som er knyttet til serviceaftaler i status Godkendt, Afventer eller Delvist godkendt, for hvilke anvendersystemet er leveret af brugerens organisation.



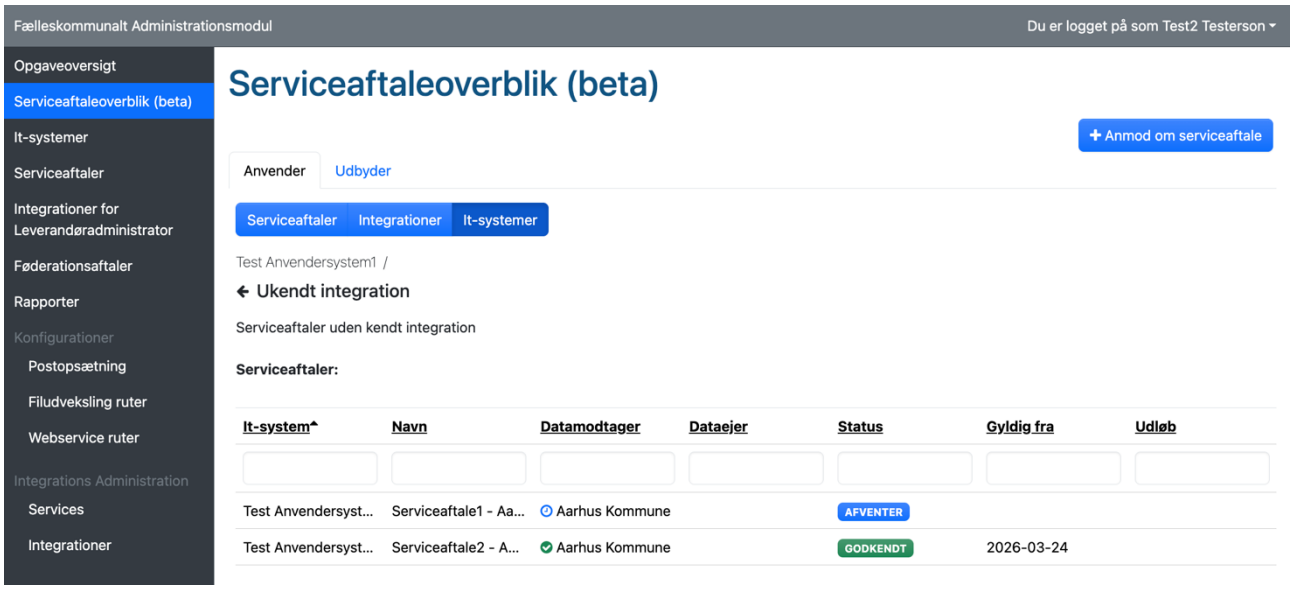
Når et element i listen aktiveres, fremkommer en side med en liste over alle de Integrationsversioner, som er knyttet til de serviceaftaler, der både opfylder ovenstående kriterier og er knyttet til det valgte It-system. For hver Integrationsversion i listen leveres i kolonnerne Godkendt og Afventende en optælling af, hvor mange af disse serviceaftaler, der er i status hhv. Godkendt eller Afventende. Serviceaftaler i status Delvist godkendt medregnes i kolonnen Afventende. Bemærk, at ældre serviceaftaler kan være knyttet til mere end én Integrationsversion, så summerne kan overstige det faktiske antal serviceaftaler.



Ved aktivering af et element i denne liste, fremkommer en side med en liste over de serviceaftaler, som opfylder ovenstående kriterier og er knyttet til den valgte Integrationsversion.



Hvis der på foregående side er valgt 'Ukendt integration' vil listen bestå af de serviceaftaler, som ikke er knyttet til nogen Integrationsversion.



Fra listen af serviceaftaler kan man vælge en specifik serviceaftale, som vises som beskrevet i afsnit 5.12.

Udbyder > Services

Denne indgang giver en liste over alle de services, som udbydes af It-systemer leveret af din organisation.



For hver service i listen kan du se

- hvilket It-system, servicen udbydes af
- hvilke ServiceMajorversioner, servicen indgår i
- hvilke Integrationsversioner, disse ServiceMajorversioner indgår i.

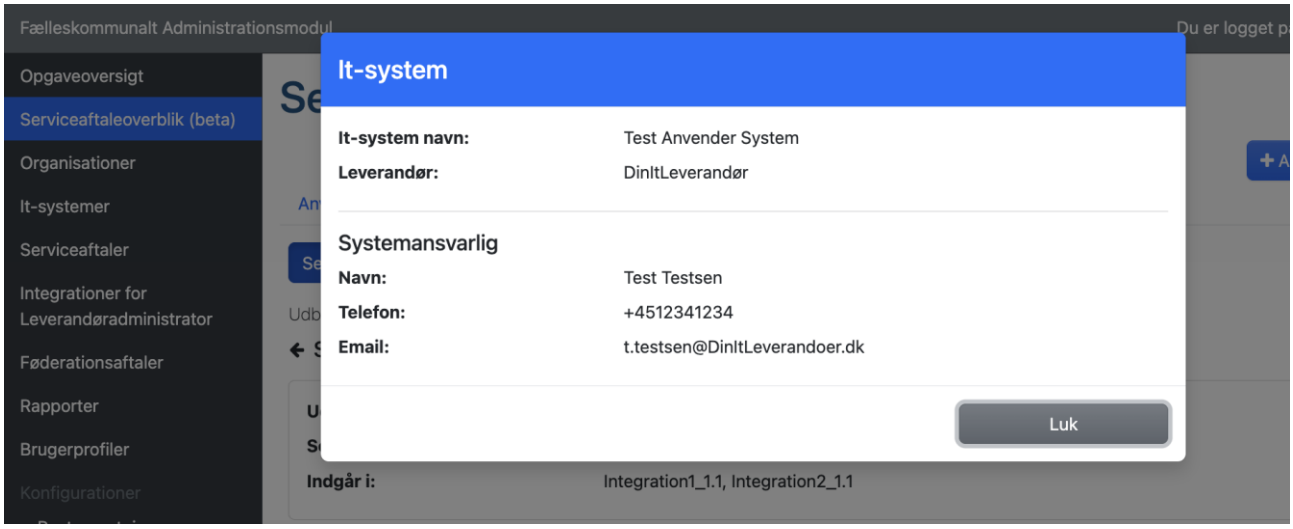
Den sidste kolonne viser en optælling af, hvor mange Anvendersystemer, der har aftaler med den pågældende service.

Ved klik på en service i listen vises flere detaljer:



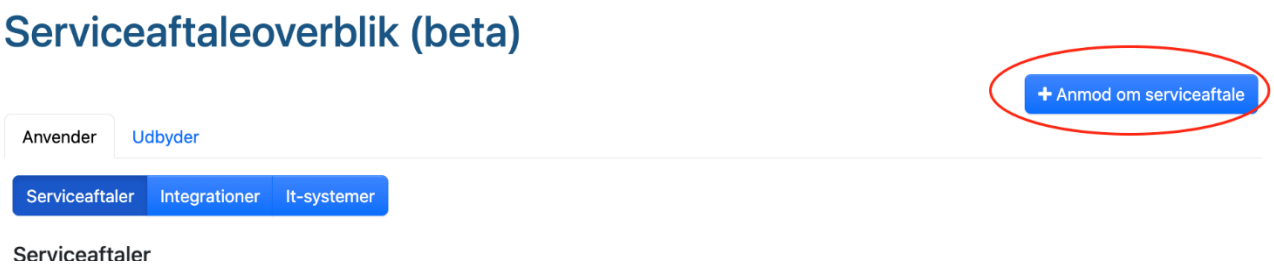
I listen nederst vises de Anvendersystemer, der har aftaler med servicen med en optælling af, hvor mange aftaler, der er tale om. Det er *ikke* muligt at få vist yderligere oplysninger om de konkrete aftaler.

Ved aktivering af et element i listen, kan man dog få vist kontaktoplysningerne for det pågældende It-system.



Anmod om serviceaftale

På alle undersider til menupunktet Serviceaftaleoverblik findes der en knap øverst til højre: ”Anmod om serviceaftale”. Denne knap aktiverer dialogen for anmodning om serviceaftale som beskrevet i afsnit 5.11.2 Anmodning ved brug af Integrationer.



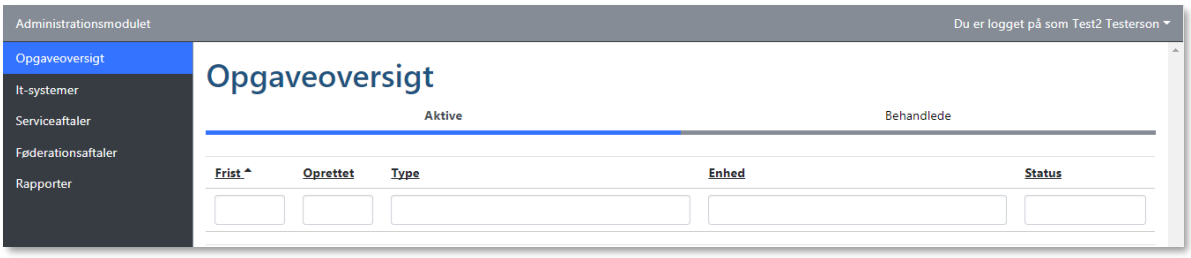
5.15 Kopier serviceaftaler

Brugeren: Med rollen Leverandøradministrator kan du kopiere en serviceaftale, som din organisation har anmodet om.

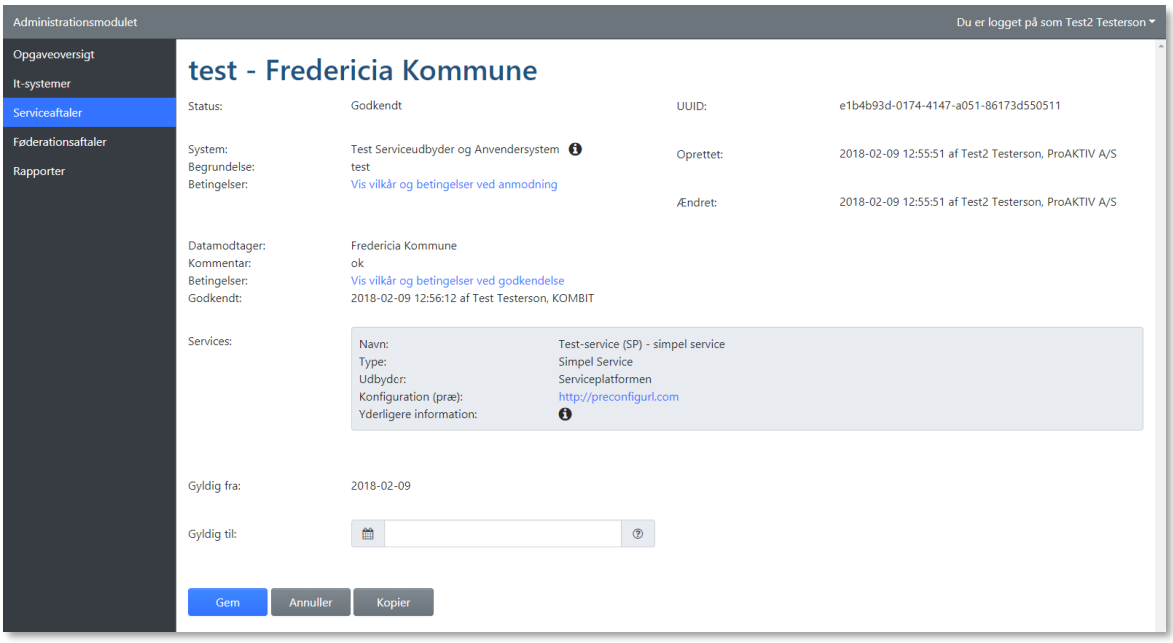
Vejledning:

1. I Administrationsmodulet skal du vælge punktet Serviceaftaler i venstremenuen. Herefter får du et overblik over serviceaftaler tilknyttet din organisation. Serviceaftalerne kan have en status ”Afventer”, ”Godkendt”, ”Afvist”, ”Udløbet” eller ”Delvis godkendt”. ”Delvis godkendt” betyder at aftalen afventer behandling fra en af de omfattede myndigheder. Du kan fremsøge en serviceaftale ved at søge i

felterne UUID, Navn, System, Dataejer, Datamodtager eller Status.

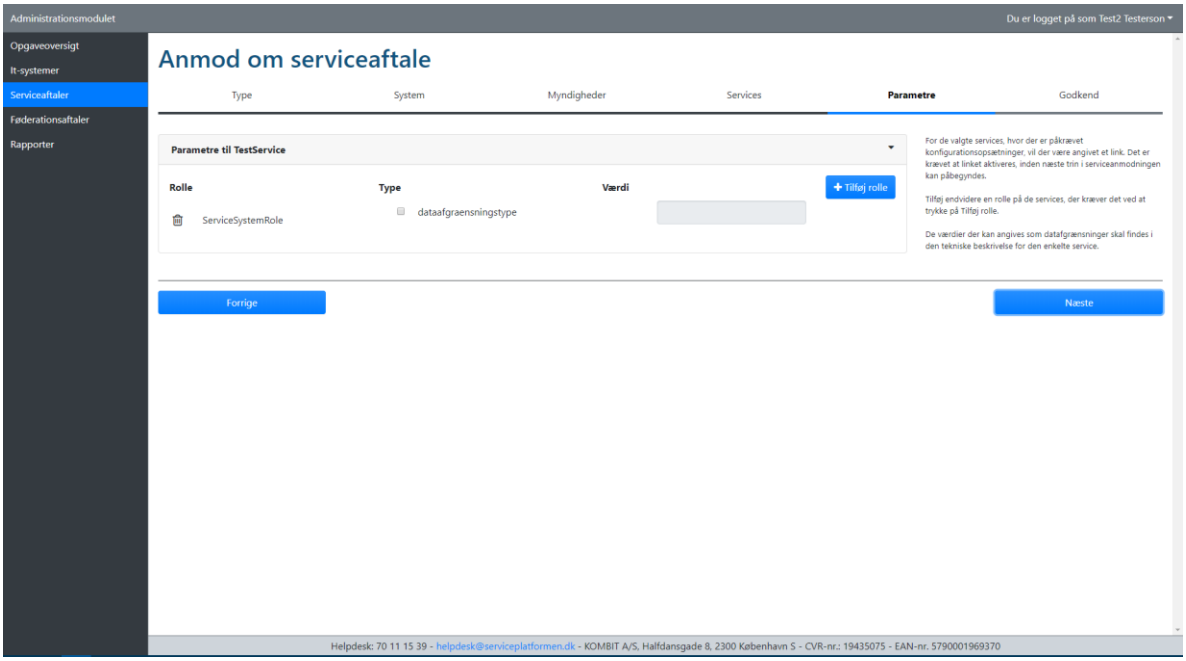


2. For at kopiere en serviceaftale, så skal du først vælge en serviceaftale fra listen ved at klikke på den. Det er lige meget hvilken status den serviceaftale du vil kopiere har, dvs. den kan have status afventer, godkendt, afvist eller delvist godkendt. Når du har åbnet en serviceaftale, skal du trykke på knappen ”Kopier”.

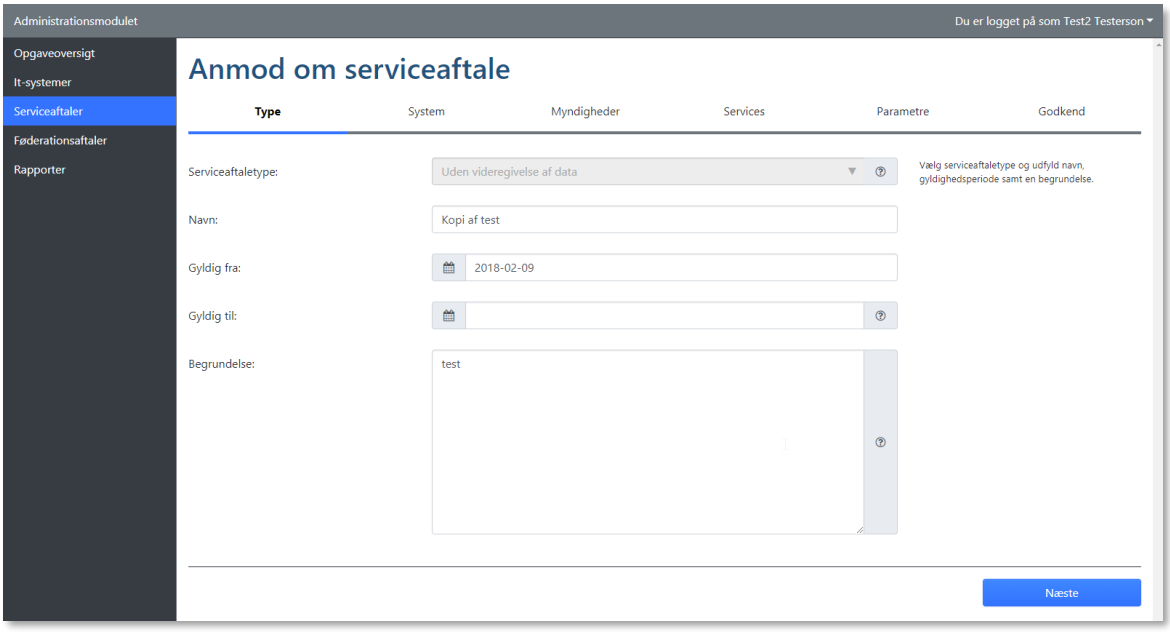


En serviceaftale kopieres i sin helhed hvis den er gyldig. Hvis hele serviceaftalen derimod ikke er gyldig, fjernes det ugyldige ved kopiering. Dette tilfælde kan eksempelvis opstå hvis en dataafgrænsningstype er blevet ændret eller fjernet fra servicesystemrollen, og derved ikke længere er gyldig på en serviceaftale. Hvis dataafgrænsningstypen er blevet fjernet fra systemrollen, fremgår den ikke længere på kopien. Ved ændring af en dataafgrænsningstype er den synlig på kopien, men skal redigeres afhængig af hvilken ændring på dataafgrænsningstypen, der er blevet foretaget således, at dataafgrænsningsværdien nu er gyldig.

Nedenstående billede er et eksempel på en kopi af en serviceaftale hvor den tilknyttede dataafgrænsningstype er blevet ændret – i dette tilfælde det regulære udtryk. Brugeren skal aktivt vælge den pågældende dataafgrænsningstype og indtaste en gyldig værdi for at fortsætte oprettelsen af kopien.



3. Når serviceaftalen er kopieret, kan du se, at navnet på den til en start er ”Kopi af [navnet på den serviceaftale du har kopieret]”. Du kan ændre navnet til, hvad du ønsker den nye serviceaftale skal hedde. I felterne for gyldighedsperiode, er gyldig fra sat til dags dato, mens sluttidspunktet ikke er udfyldt. Du kan tilrette gyldighedsperioden til, hvad du ønsker.



4. Gennemgå de seks trin for anmodning om serviceaftalen, Type, System, Myndighed, Services, Parametre og Godkend. Hvis der er behov for det, så tilret anmodningen. Se evt. nærmere beskrivelse om de seks trin i afsnit 5.11 ”Anmod om serviceaftale”. Når den nye aftale er gemt, kan den ikke længere ændres.

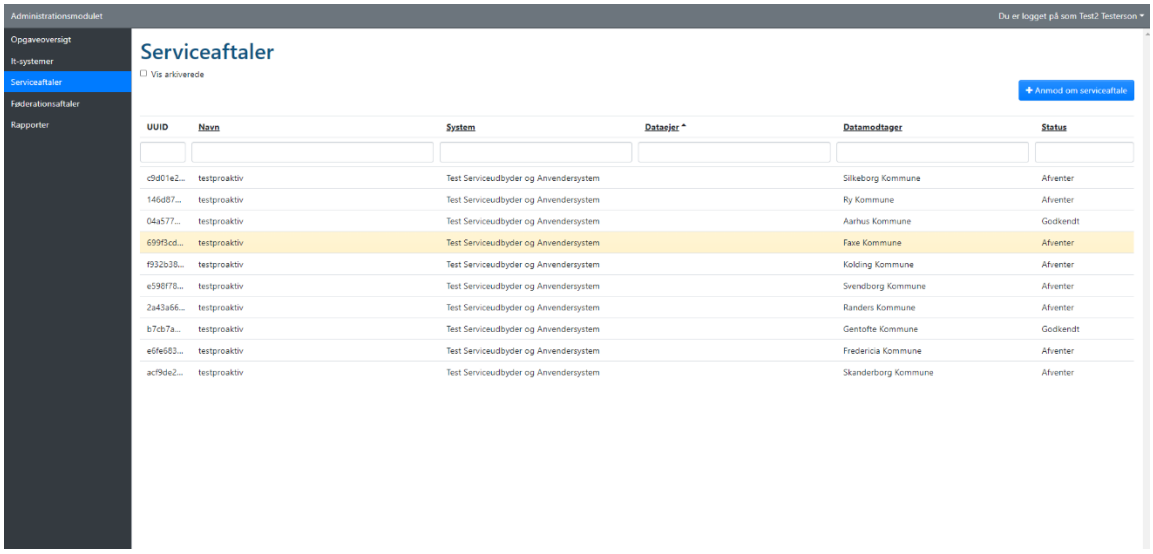
Resultat: Du har taget en kopi af en serviceaftale, som du kan bruge til at anmode om en ny serviceaftale.

5.16 Tilbagekald serviceaftale

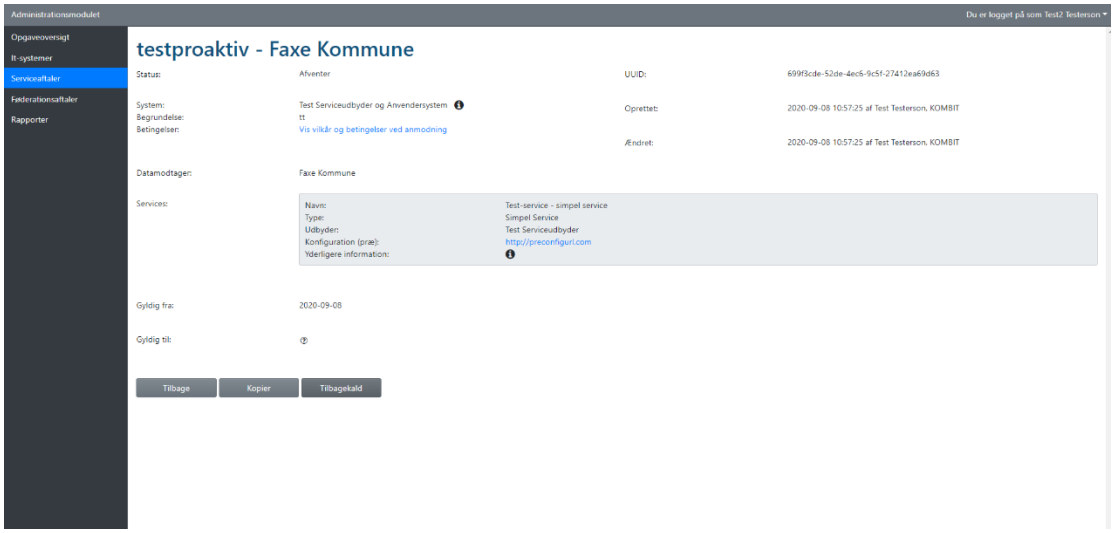
Brugeren: Med rollen leverandøradministrator kan du tilbagekalde en oprettet serviceaftale anmodning.

Vejledning:

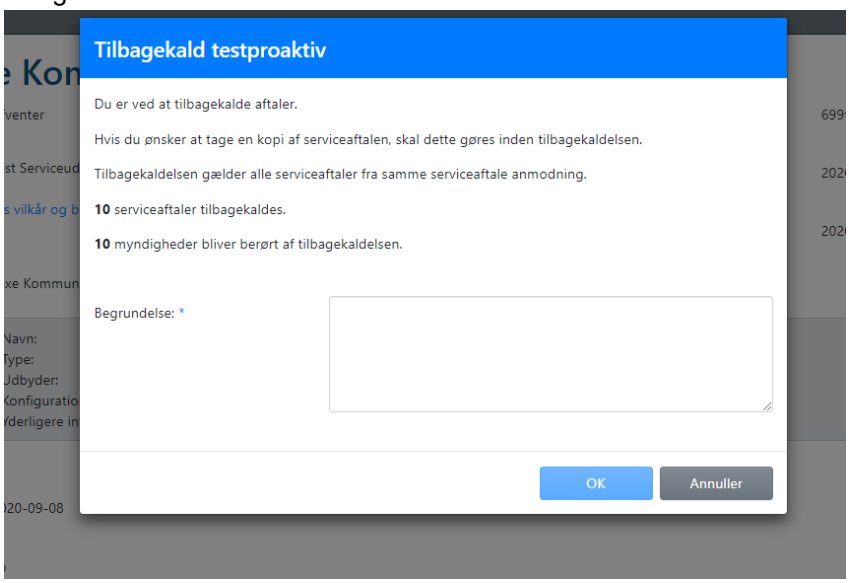
1. I Administrationsmodulet skal du vælge punktet Serviceaftaler i venstremenuen. Herefter får du det overblik over serviceaftaler tilknyttet din organisation. Serviceaftalerne kan have status ”Afventer”, ”Godkendt”, ”Afvist” eller ”Delvist godkendt”. ”Delvist godkendt” betyder, at aftalen afventer behandling fra en af de omfattede myndigheder.
   Du kan fremsøge en serviceaftale ved at søge i felterne UUID, Navn, System, Dataejer, Datamodtager og Status. Vælg en serviceaftale fra listen ved at klikke på den.



2. Når du har valgt en aftale med en af statusserne, har du mulighed for at tilbagekalde Serviceaftalen. Du tilbagekalder aftalen ved at trykke på knappen tilbagekald. Serviceaftalen kan tilbagekaldes uanset om status er ”Afventer”, ”Godkendt”, ”Afvist” eller ”Delvist godkendt”.



3. Følgende advarsel vises til brugeren som giver brugeren et overblik over omfanget af tilbagekaldelsen.



Antal berørte myndigheder er antallet af myndigheder som er en del af serviceaftalerne, enten som datamodtager eller dataejer.

Begrundelse er obligatorisk for tilbagekaldelsen.

Leverandøren kan med fordel kopiere en aftale inden tilbagekaldelse, såfremt denne følger navngivningsvalideringen beskrevet under Anmod om Serviceaftale afsnittet.

Hvis præcis samme navngivning ønskes, men ikke er mulig i forhold til navngivningsvalideringen, bør aftalerne tilbagekaldes, og en ny anmodning oprettes.

Tilbagekaldte serviceaftaler kan fremsøges i arkivet, og kan bruges som hjælp til en ny anmodning da disse kan åbnes i nye faner og vinduer.

Resultat: Serviceaftalerne tilbagekaldes fra dags dato og kan findes i arkivet.

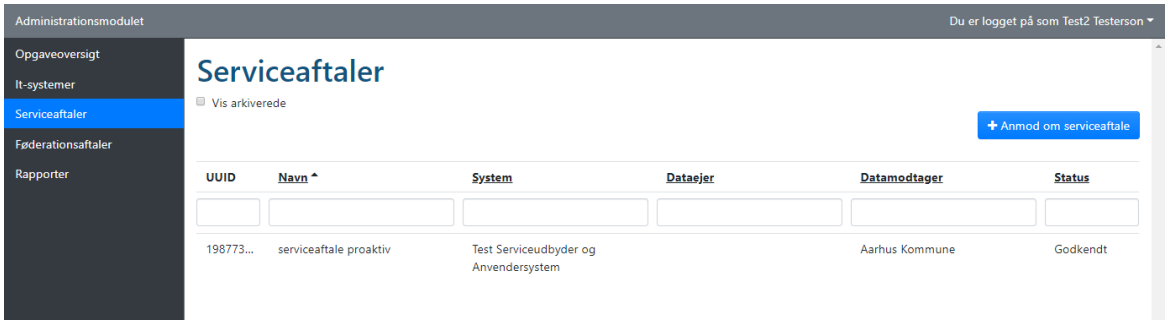
5.17 Opsig serviceaftale

Brugeren: Med rollen leverandøradministrator kan du opsige en tidligere godkendt serviceaftale.

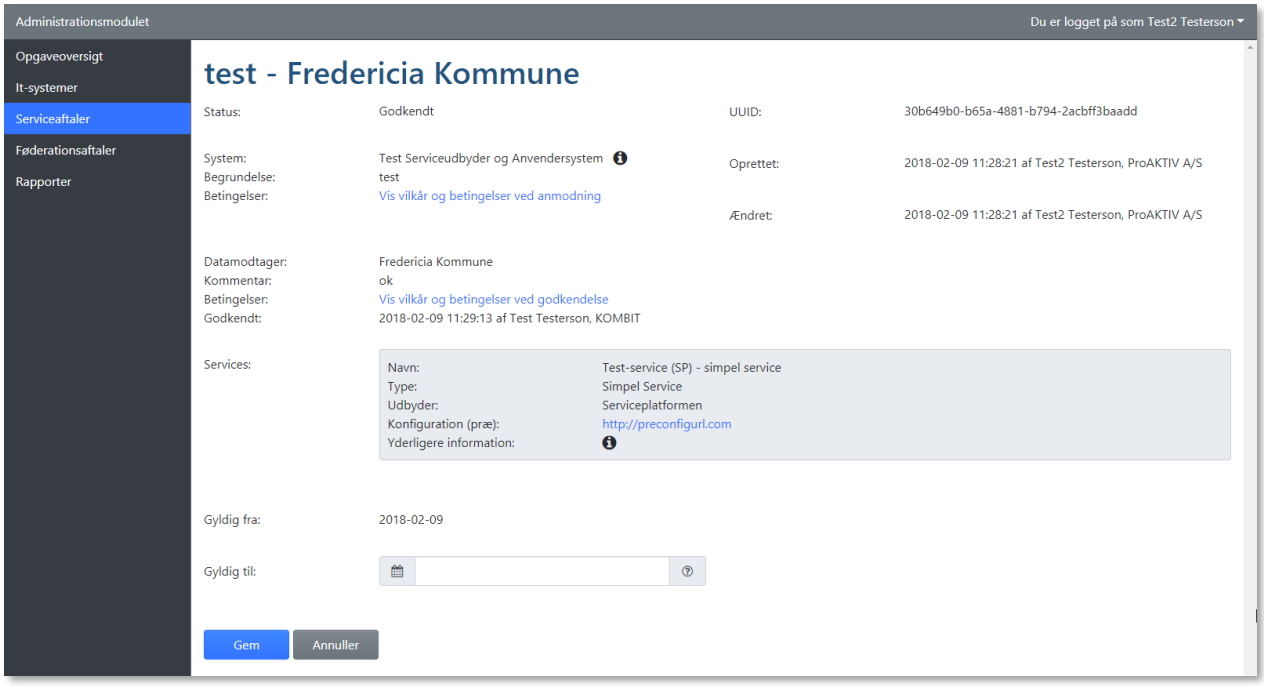
Vejledning:

1. I Administrationsmodulet skal du vælge punktet Serviceaftaler i venstremenuen. Herefter får du et overblik over serviceaftaler tilknyttet din organisation. Serviceaftalerne kan have status ”Afventer”, ”Godkendt”, ”Afvist” eller ”Delvist godkendt”. ”Delvist godkendt” betyder, at aftalen afventer behandling fra en af de omfattede myndigheder.
   Du kan fremsøge en serviceaftale ved at søge i felterne UUID, Navn, System, Dataejer, Datamodtager og Status. Vælg en serviceaftale fra listen ved at klikke på den.

2.



Når du har valgt en aftale med status ”Godkendt”, har du mulighed for at opsige Serviceaftalen. Du opsiger aftalen ved at vælge, hvornår opsigelsen skal gælde fra ved at tilføje eller ændre datoen for ”Gyldig til”. Hvis datoen allerede er sat, kan den kun ændres til en tidligere dato, dog tidligst dagen efter dags dato. Når datoen for ”Gyldig til” er overskredet er serviceaftalen ikke længere aktiv og vil blive arkiveret. Du kan stadig se aftalen på oversigten over serviceaftaler, hvis du trykker ”Vis arkiverede”, den vil have status ”Udløbet”.



Resultat: Serviceaftalen er opsagt fra den angivet dato i feltet ”Gyldig til”.

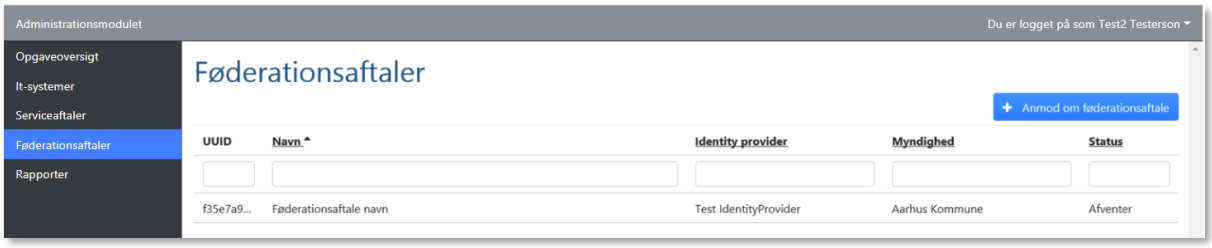
5.18 Anmod om føderationsaftale

Brugeren: Med rollen Leverandøradministrator kan du anmode om en føderationsaftale. Aftalen giver Identity Provideren ret til at udstede tokens, der bevidner, at brugere er autentificeret i kontekst af den myndighed, der har godkendt aftalen. Dette token anvendes til at afgøre, hvorvidt en given bruger får adgang til et Brugervendt system på vegne af denne myndighed.

Bemærk: Som it-leverandør skal du have tilsluttet dit it-system som Identity Provider til Rammearkitekturen.

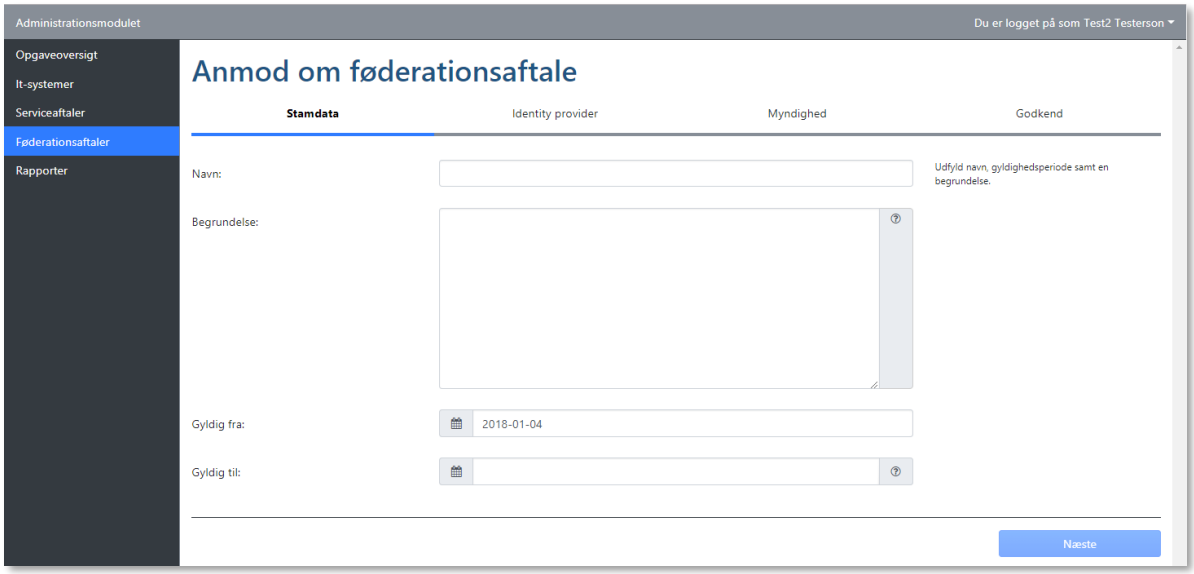
Vejledning:

1. I Administrationsmodulet skal du vælge punktet Føderationsaftaler i venstremenuen. Herfra får du overblik over føderationsaftaler, der allerede er anmodet om. Du kan fremsøge en føderationsaftale ved at søge i felterne UUID, Navn, Identity Provider, Myndighed og Status. Vælg en føderationsaftale ved at klikke på den fra listen.



2. For at anmode om en føderationsaftale, skal du trykke på knappen ”Anmod om føderationsaftale”. Herefter skal du igennem fire trin for at gennemføre anmodningen: Stamdata, Identity Provider, Myndighed og Godkend.

3. Stamdata

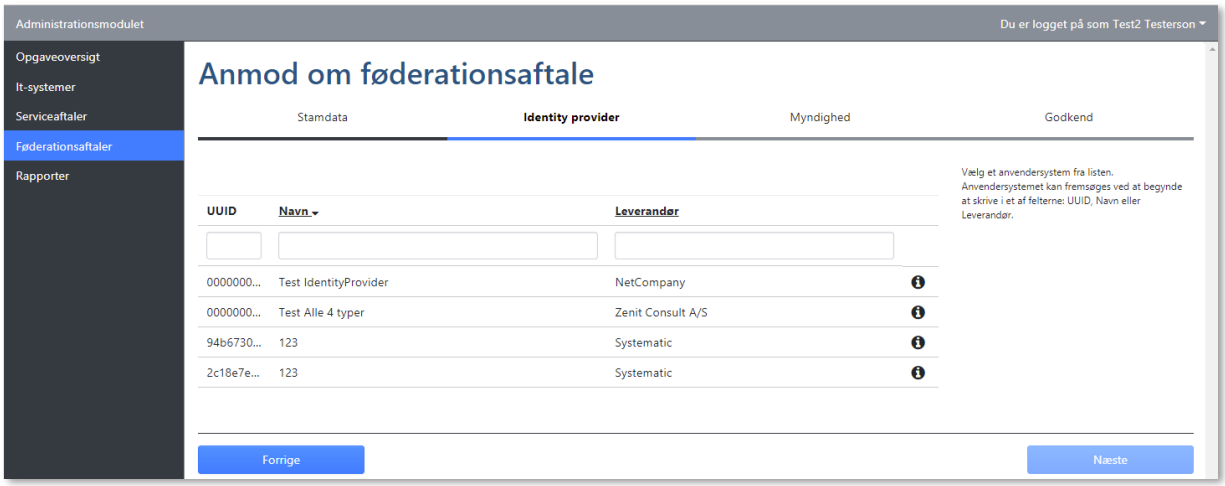


Udfyld følgende oplysninger for Stamdata:

- Navn: Giv føderationsaftalen et sigende navn.
- Begrundelse: Tilføj begrundelse for anmodningen om serviceaftalen. Begrundelsen ses når myndigheden skal godkende anmodningen.
- Gyldig fra: Udfyld hvornår aftalen skal være gyldig fra.
- Gyldig til: Udfyld evt. hvornår aftalen skal være gyldig til. Det er ikke krævet at gyldig til udfyldes det kan man tilføje senere, hvis der er behov for det.

Fortsæt til trin 2 – Identity Provider ved at tykke på ”Næste”.

4. Identity provider

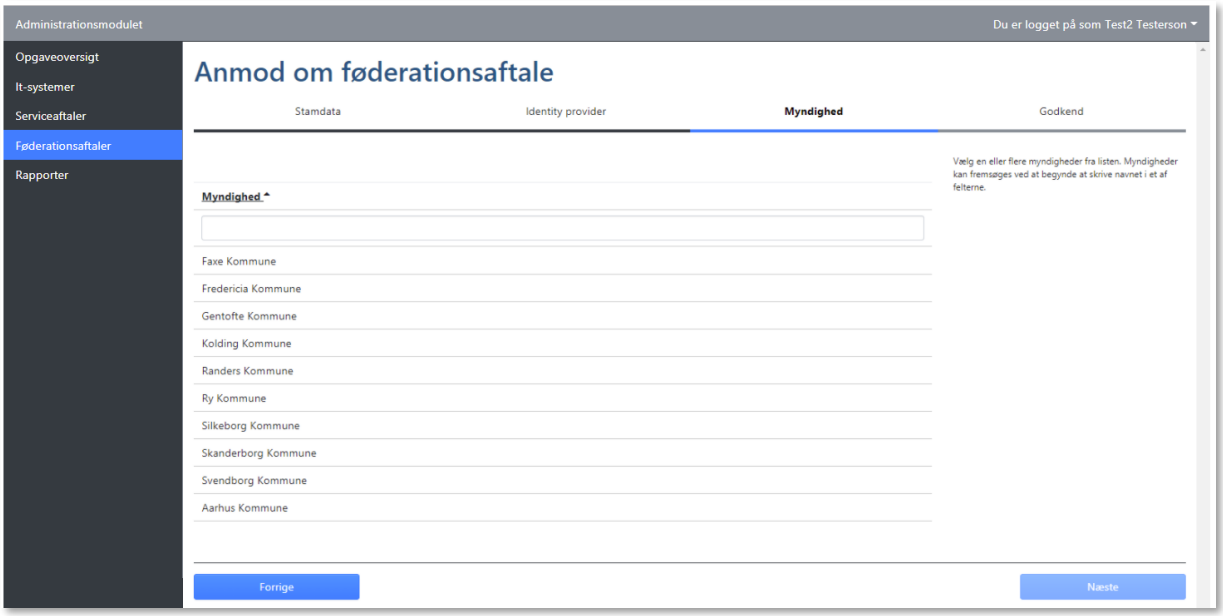


Under trin 2 – Identity provider – skal du vælge en Identity provider. Du kan fremsøge en Identity provider i felterne UUID, Navn og Leverandør. Vælg et system fra listen ved at klikke på det.

For yderligere information for den enkelte Identity provider kan du klikke på i'et i listen ud for hver Identity provider.

Fortsæt til trin 3 – Myndighed ved at trykke på "Næste".

5. Myndighed



Under trin 3 – Myndighed – skal du vælge den myndighed, som aftalen skal indgås med. Du kan fremsøge en myndighed i feltet Myndighed. Vælg myndigheden ved at klikke på den fra listen. Bemærk at data ikke kan tilgås før myndigheden har godkendt føderationsaftalen.

Fortsæt til trin 4 – Godkend ved at trykke på "Næste".

6. Godkend



Under trin 4 – Godkend – skal du læse anmodningen igennem og klikke på linket ”Accepter vilkår og betingelser”. Læs vilkår og betingelserne og accepter dem for at kunne færdiggøre anmodningen. Afslut med at trykke på ”Færdig”.

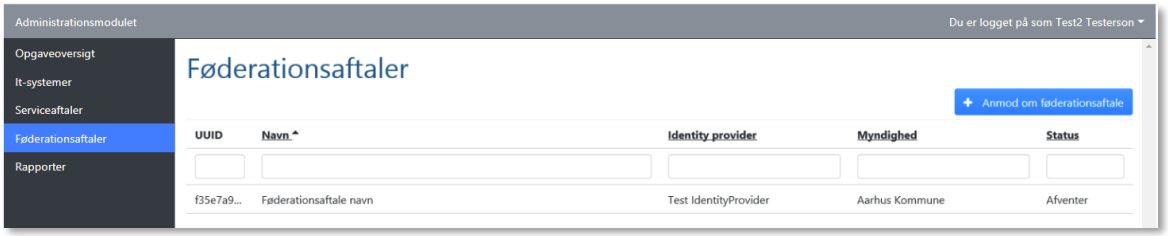
Resultat: Anmodningen om føderationsaftalen er sendt til godkendelse hos den valgte myndighed.

5.19 Vis føderationsaftale

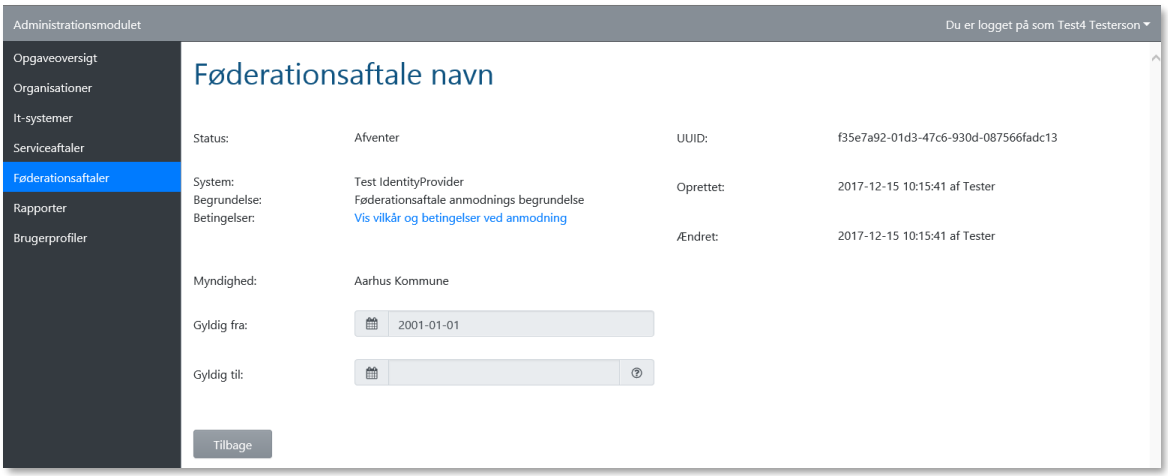
Brugeren: Med rollen Leverandøradministrator kan du få vist de føderationsaftaler, som din organisation har anmodet om.

Vejledning:

1. I Administrationsmodulet skal du vælge punktet Føderationsaftaler i venstremenuen. Herefter får du et overblik over føderationsaftaler tilknyttet din organisation. Føderationsaftalerne kan have en status ”Afventer”, ”Godkendt” eller ”Afvist”. Du kan fremsøge en føderationsaftale ved at søge i felterne UUID, Navn, Identity provider, Myndighed eller Status. Vælg en føderationsaftale fra listen ved at klikke på den.



2. Når du har valgt en aftale, kan du se de detaljer, som er tilknyttet aftalen.



Det er kun muligt at redigere "Gyldig til" datoen. Hvis der allerede står en dato i feltet, kan den kun ændres til en tidligere dato, dog tidligst dagen efter dags dato. Når datoen for "Gyldig til" er overskredet, er føderationsaftalen ikke længere aktiv og vil blive arkiveret.

- Status: Her vises status for føderationsaftalen.
- System: Her vises fra hvilken Identity Provider, anmodningen om føderationsaftalen kommer fra.
- Begrundelse: Her vises it-leverandørens begrundelse for anmodningen om føderationsaftalen
- Betingelser: Her vises vilkår og betingelser som it-leverandøren har godkendt i forbindelse med anmodningen.
- Myndighed: Den myndighed der har godkendt/afvist aftalen.

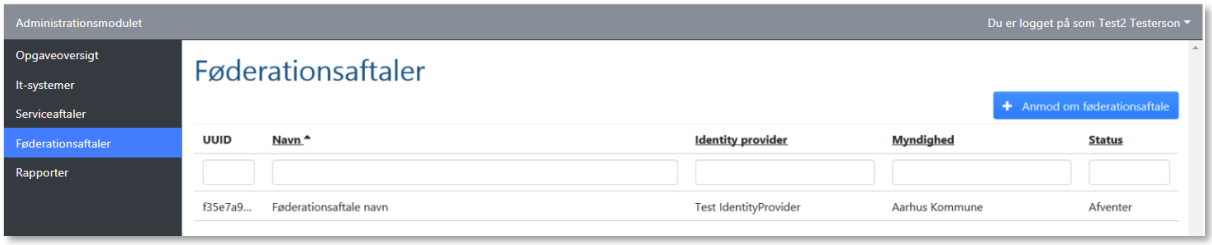
Resultat: Du har nu fået vist de føderationsaftaler, der er tilknyttet din organisation.

5.20 Opsig føderationsaftale

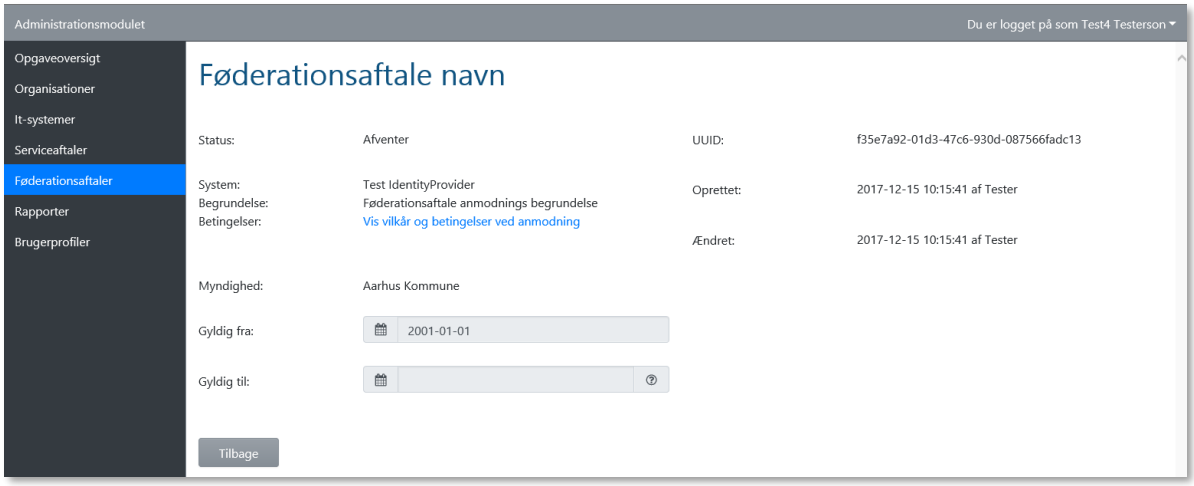
Brugeren: Med rollen Leverandøradministrator kan du opsige en tidligere godkendt føderationsaftale.

Vejledning:

1. I Administrationsmodulet skal du vælge punktet Føderationsaftaler i venstremenuen. Herefter får du et overblik over serviceaftaler tilknyttet din organisation. Føderationsaftalerne kan have en status "Afventer", "Godkendt", "Afvist" eller "Delvist godkendt". "Delvis godkendt" betyder at aftalen afventer behandling fra den omfattede myndighed. Du kan fremsøge en føderationsaftale ved at søge i felterne UUID, Navn, Identity Provider, Myndighed eller Status. Vælg en føderationsaftale fra listen ved at klikke på den.



2. Når du har valgt en aftale med status ”Godkendt”, har du mulighed for at opsige føderationsaftalen.



Du opsiger aftalen ved at tilføje eller ændre datoen for ”Gyldig til”. Hvis datoen allerede er sat, kan den kun ændres til en tidligere dato, dog tidligst dagen efter dags dato. Når datoen for ”Gyldig til” er overskredet, er føderationsaftalen ikke længere aktiv og vil blive arkiveret. Du vil ikke længere have mulighed for at se aftalen.

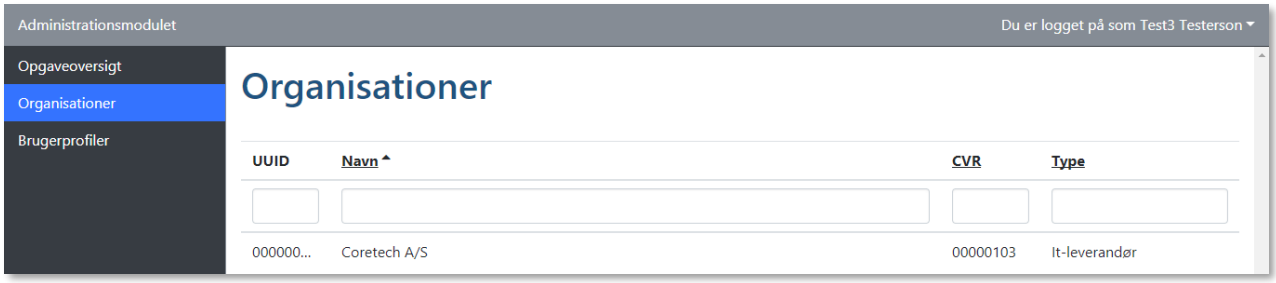
Resultatet: Føderationsaftalen er opsagt fra den angivet dato i feltet ”Gyldig til”.

5.21 Vis, rediger eller slet en organisation

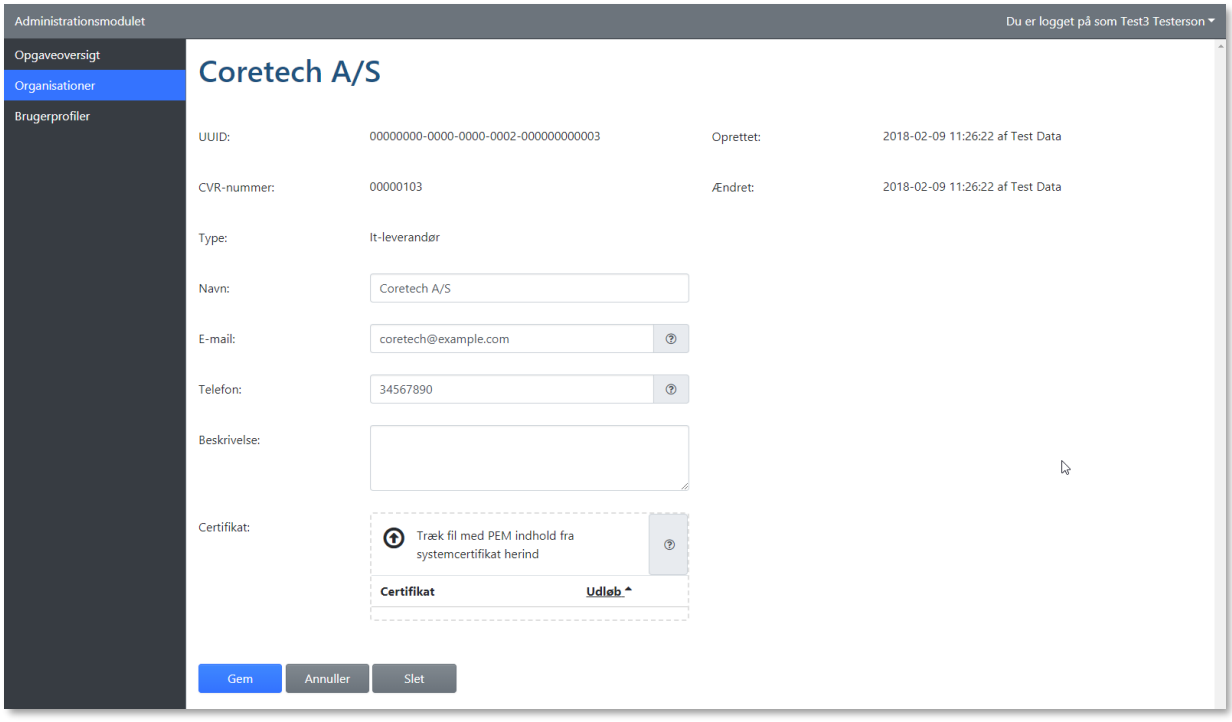
Brugeren: Med rollen Organisationsadministrator kan du få vist din organisation, redigere stamdata eller slette organisationen.

Vejledning:

1. I Administrationsmodulet skal du vælge punktet Organisationer i venstremenuen. Herefter får du vist din organisation på listen. For at se flere oplysninger om din organisation skal du vælge den fra listen ved at klikke på den.



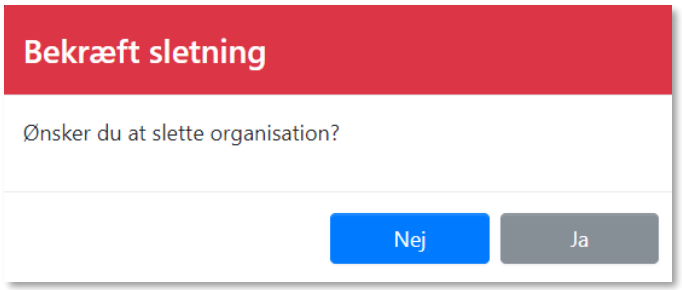
2. Herefter kan du se stamoplysninger for din organisation.



Du kan redigere Navn, E-mail, Telefon, Beskrivelse og Certifikat. Certifikatet skal du bruge, når du ønsker at anvende Administrationsmodulets eksterne snitflade. Certifikaterne kan bruges til at få adgang til administrations-API'en og til at få adgang til Attribut-tjenesten på Context Handler. Hvis certifikatet skal bruges til at få adgang til Attribut-tjenesten, skal CVR-nummeret i certifikatet stemme overens med organisationens eget CVR-nummer. Afslut med at trykke "Gem". Hvis der findes opgaver relateret til organisationen, som ikke er udført, vises en dialog, hvor det er muligt at markere opgaverne som udført.

Se afsnit 5.6 punkt 4 for mere information. Du vil efterfølgende komme tilbage til listevisningen.

3. Ønsker du at slette din organisation, trykker du på knappen ”Slet”. Funktionen er kun relevant hvis organisationen nedlægges. Vær opmærksom på, at en organisation ikke kan slettes, hvis den har tilsluttet anvendersystemer, jobfunktionsroller, føderationsaftale eller hvis den er part i en serviceaftale. Når du sletter en organisation, får du nedenstående meddelelse op, hvor du skal bekræfte, at du vil slette organisationen. Hvis du siger ”Ja” bliver din organisation slettet, og du kommer tilbage til listevisningen.



Resultat: Hvis du har lavet ændringer, er stamoplysningerne nu opdateret. Hvis du har slettet en organisation, er den nu fjernet fra Administrationsmodulet.

Vær opmærksom på at hvis du ønsker din organisation slettet på Serviceplatformen, skal du skrive til Serviceplatformens Helpdesk på helpdesk@serviceplatformen.dk.

5.22 Rapporter

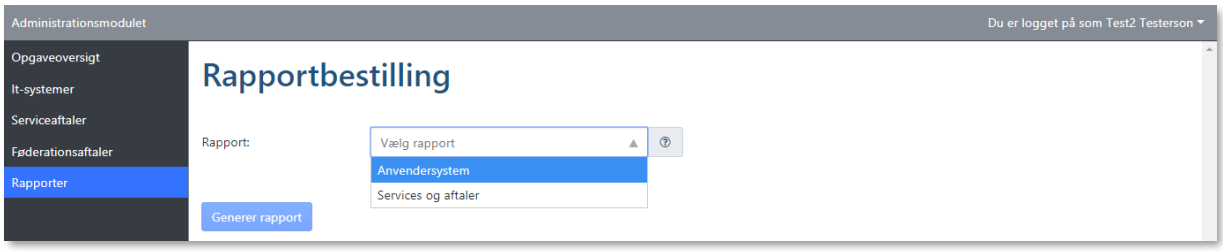
Brugeren: Med rollen Leverandøradministrator kan du trække fem typer rapporter fra Administrationsmodulet. De fem rapporter er ”Anvendersystem”, ”Services og aftaler”, ”Services og aftaler med integrationer”, ”Brugersystemroller” og ”Certifikater”. Du kan bruge rapporterne til videre analyse f.eks. til at finde manglende serviceaftaler eller til at finde bestemte konfigurationsfejl. De fem rapporter gennemgås enkeltvis i nedenstående.

Rapport: ”Anvendersystem”. Rapporten viser, hvilke services et anvendersystem har serviceaftaler med. Du kan kun se de data, der er relateret til din egen organisation, dvs. du kan kun se de anvendersystemer, som din organisation har oprettet.

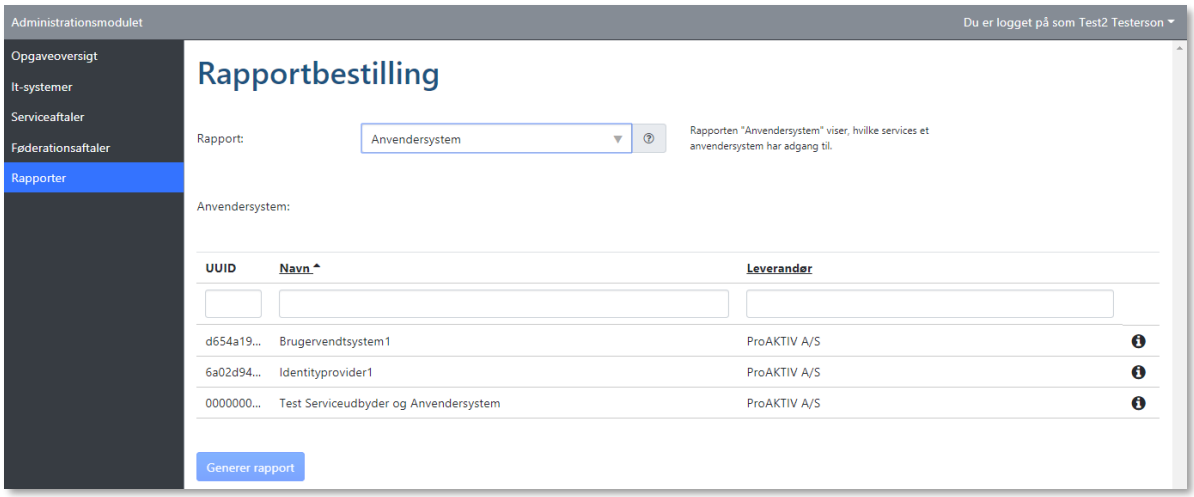
Vejledning:

1. I Administrationsmodulet skal du vælge punktet Rapporter i venstremenuen. Herefter skal du fra dropdown-listen vælge, hvilken rapporter du ønsker at generere.

2. Vælg rapporten ”Anvendersystem” fra listen

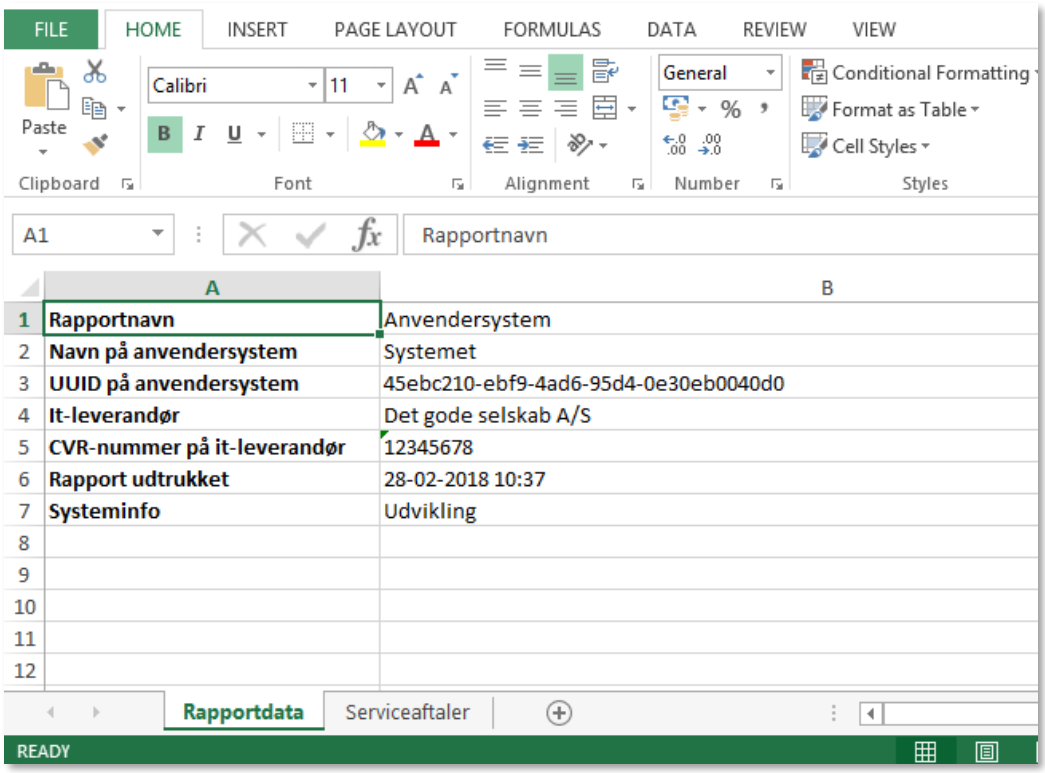


3. Vælg hvilket anvendersystem, du ønsker at se data fra, og afslut med at trykke på knappen ”Generer rapport”. Rapporten har filtypen .xlsx.



4. Rapporten modtages i browseren og kan åbnes i Excel direkte, eller ved at gemme den først og herefter åbne den.

5. Rapporten ”Anvendersystem” indeholder to faneblade i Excel-arket, ”Rapportdata” og ”Serviceaftaler”.



Fanen ”Rapportdata” indeholder følgende informationer:

- Rapportnavn: For denne rapport står der ”Anvendersystem”.
- Navn på anvendersystem
- UUID på anvendersystem
- It-leverandør
- CVR-nummer på it-leverandør
- Rapport udtrukket: Her vises dato og tidspunkt for hvornår rapporten er udtrukket.
- Systeminfo: Her vises på hvilket miljørapporten er udtrukket.

Fanen ”Serviceaftaler” indeholder følgende kolonner:

- SP Snitflade
- Navn på service på Serviceplatformen
- EntityId for service på Serviceplatformen
- Roller og dataafgrænsninger for service på Serviceplatformen
- Navn for service på serviceudbyder
- EntityId for service på serviceudbyder
- Roller og dataafgrænsninger for service på serviceudbyder
- Serviceudbyder
- UUID på serviceudbyder
- Dataejer (myndighed)
- CVR-nummer på dataejer
- Datamodtager (myndighed)
- CVR-nummer på datamodtager

- Serviceaftale
- UUID på serviceaftale
- Status på serviceaftale

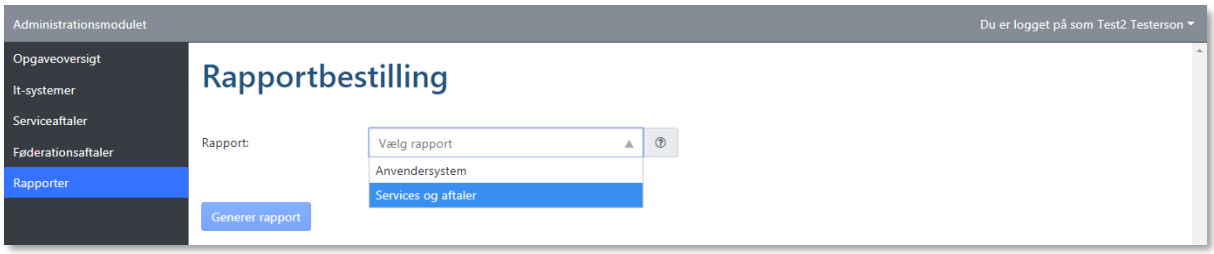
Resultat: Du har fået vist rapporten ”Anvendersystem”.

Rapport: ”Services og aftaler”. Rapporten viser lister over services inkl. deres UUID og en kort beskrivelse.

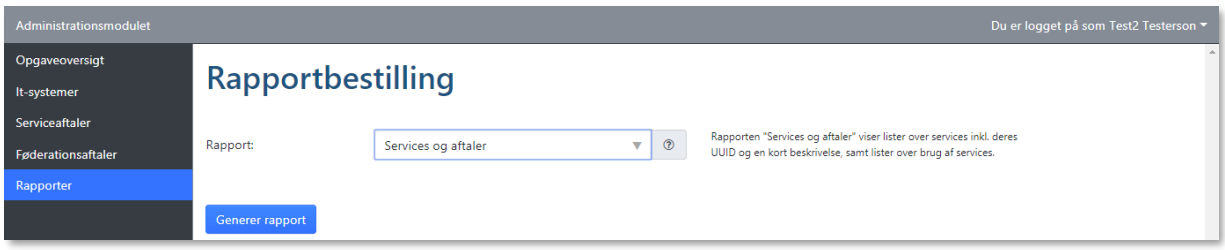
Vejledning:

1. I Administrationsmodulet skal du vælge punktet Rapporter i venstremenuen. Herefter skal du fra dropdown-listen vælge, hvilken rapporter du ønsker at generere.

2. Vælg rapporten ”Services og aftaler” fra listen

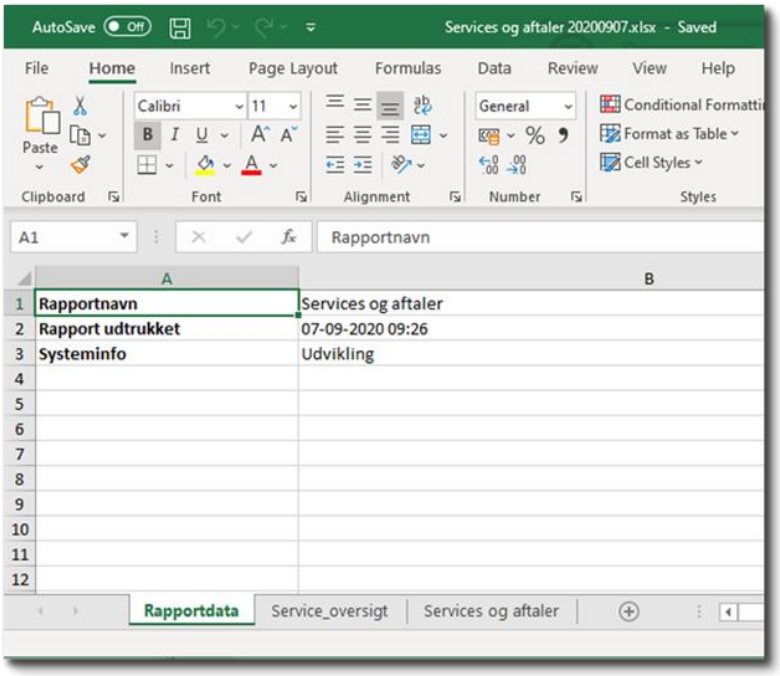


3. Tryk på knappen ”Generer rapport”. Rapporten har filtypen .xlsx.



4. Rapporten modtages i browseren og kan åbnes i Excel direkte, eller ved at gemme den først og herefter åbne den.

   Rapporten ”Services og aftaler” indeholder tre faneblade i Excel-arket, ”Rapportdata”, ” Service_oversigt” og ”Services og aftaler”.



Fanen ”Rapportdata” indeholder følgende informationer:

- Rapportnavn: For denne rapport står der ”Services og aftaler”
- Rapport udtrukket: Her vises dato og tidspunkt for hvornår rapporten er udtrukket
- Systeminfo: Her vises på hvilket miljø, rapporten er udtrukket.

Systeminfo: Her vises på hvilket miljø, rapporten er udtrukket.

Fanen ”Service_oversigt” indeholder følgende kolonner:

- Service
- Service type
- Entity id
- Beskrivelse
- Udstillet service
- Tilkoblet service
- Servicesystemrolle + dataafgrænsningstype navn

Fanen ”Services og aftaler” indeholder følgende kolonner:

- Leverandør
- Systemet som produkt (Navn)
- Systemet som produkt (UUID)
- Anvendersystem navn
- Anvendersystem uuid
- Serviceaftale navn
- Serviceaftale uuid
- Service navn
- Service entity id
- Service uuid
- Roller og dataafgrænsninger for service

- Dataejer (myndighed)
- CVR-nummer på dataejer
- Datamodtager (myndighed)
- CVR-nummer på datamodtager
- Serviceaftale status
- Serviceaftale oprettelsesdato
- Serviceaftale ændringsdato
  Serviceaftale gyldig til dato

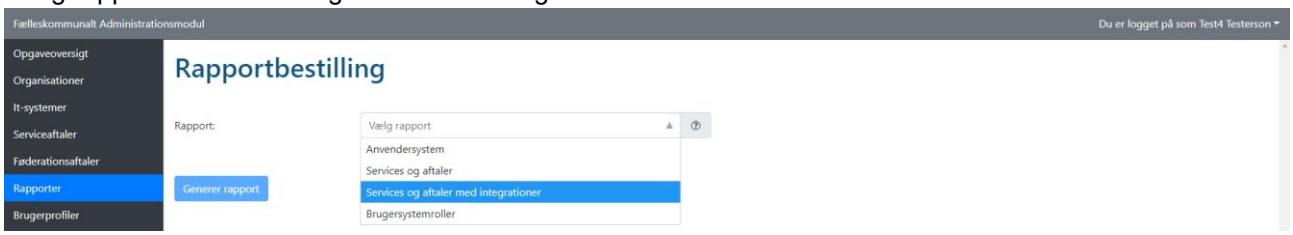
Resultat: Du har fået vist rapporten ”Services og aftaler”.

Rapport: ”Services og aftaler med integrationer”. Rapporten er en kopi af ”Services og aftaler” med udvidet data omkring integrationer.

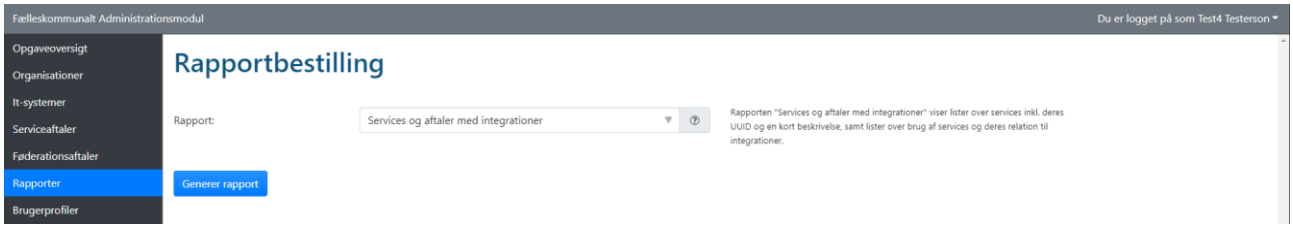
Vejledning:

1. I Administrationsmodulet skal du vælge punktet Rapporter i venstremenuen. Herefter skal du fra dropdown-listen vælge, hvilken rapport du ønsker at generere.

2. Vælg rapporten ”Services og aftaler med integrationer” fra listen

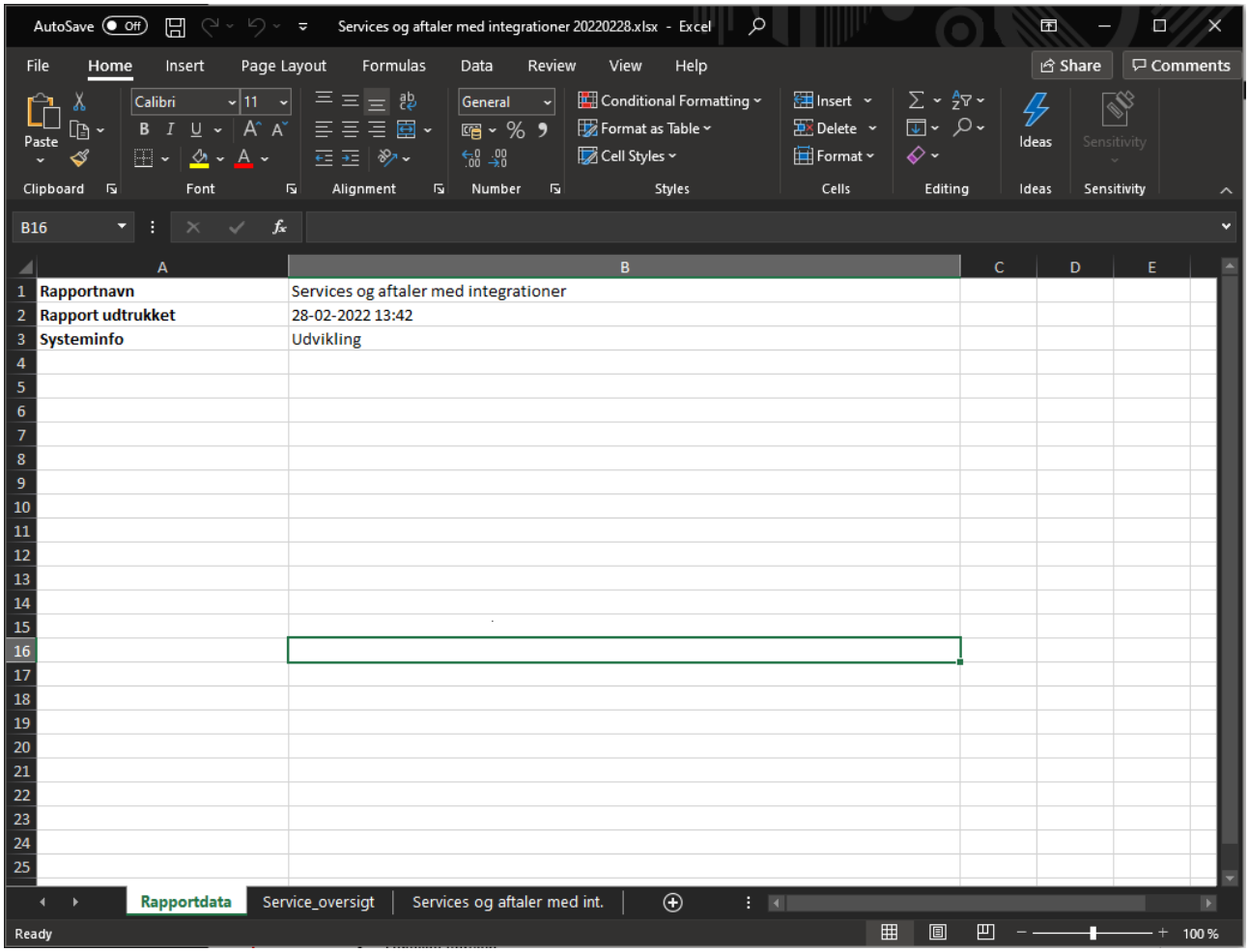


3. Tryk på knappen ”Generer rapport”. Rapporten har filtypen .xlsx.



4. Rapporten modtages i browseren og kan åbnes i Excel direkte, eller ved at gemme den først og herefter åbne den.

   Rapporten ”Services og aftaler med integrationer” indeholder tre faneblade i Excel-arket, ”Rapportdata”, ” Service_oversigt” og ”Services og aftaler med int.”.



Fanen ”Rapportdata” indeholder følgende informationer:

- Rapportnavn: For denne rapport står der ”Services og aftaler med integrationer”
- Rapport udtrukket: Her vises dato og tidspunkt for hvornår rapporten er udtrukket
- Systeminfo: Her vises på hvilket miljø, rapporten er udtrukket.

Fanen ”Service_oversigt” indeholder følgende kolonner:

- Service
- Service type
- Entity id
- Beskrivelse
- Udstillet service
- Tilkoblet service
- Servicesystemrolle + dataafgrænsningstype navn

Fanen ”Services og aftaler med int.” indeholder følgende kolonner:

- Leverandør
- Systemet som produkt (Navn)
- Systemet som produkt (UUID)
- Anvendersystem navn
- Anvendersystem uuid

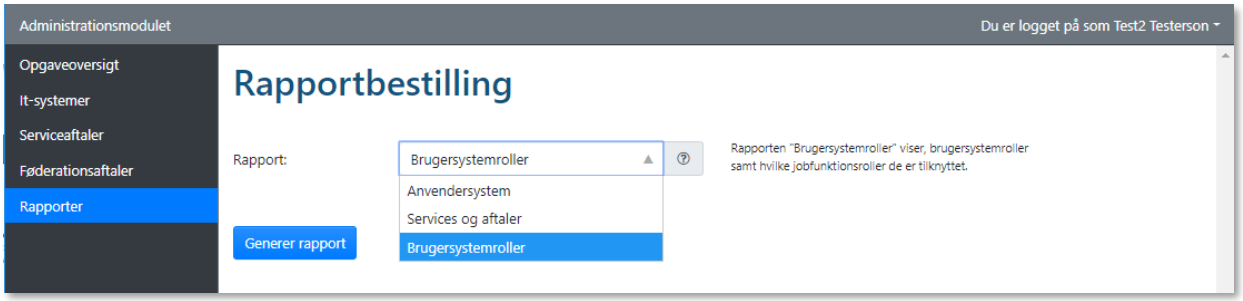
- Serviceaftale navn
- Serviceaftale uuid
- Service navn
- Service entity id
- Service uuid
- Roller og dataafgrænsninger for service
- ServiceMajorversion
- Integrationsversion
- Integrationsnummer
- Integrationstitel
- Dataejer (myndighed)
- CVR-nummer på dataejer
- Datamodtager (myndighed)
- CVR-nummer på datamodtager
- Serviceaftale status
- Serviceaftale oprettelsesdato
- Serviceaftale ændringsdato
- Serviceaftale gyldig til dato

Resultat: Du har fået vist rapporten ”Services og aftaler med integrationer”.

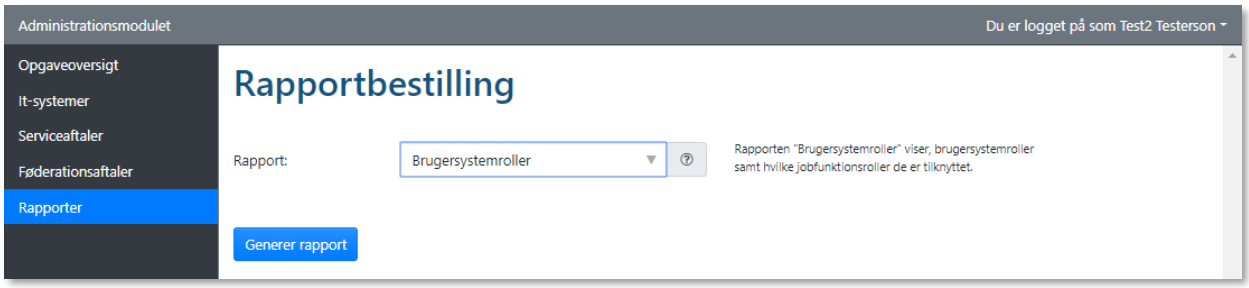
Rapport: ”Brugersystemroller”. Rapporten viser lister af brugersystemroller for leverandørers brugervendte systemer inkl. deres UUID, EntityId, og hvilke jobfunktionsroller, dataafgrænsninger og myndigheder de er tilknyttet.

Vejledning:

1. I Administrationsmodulet skal du vælge punktet Rapporter i venstremenuen. Herefter skal du fra dropdown-listen vælge, hvilken rapport du ønsker at generere, i dette tilfælde skal du vælge ”Brugersystemroller”.

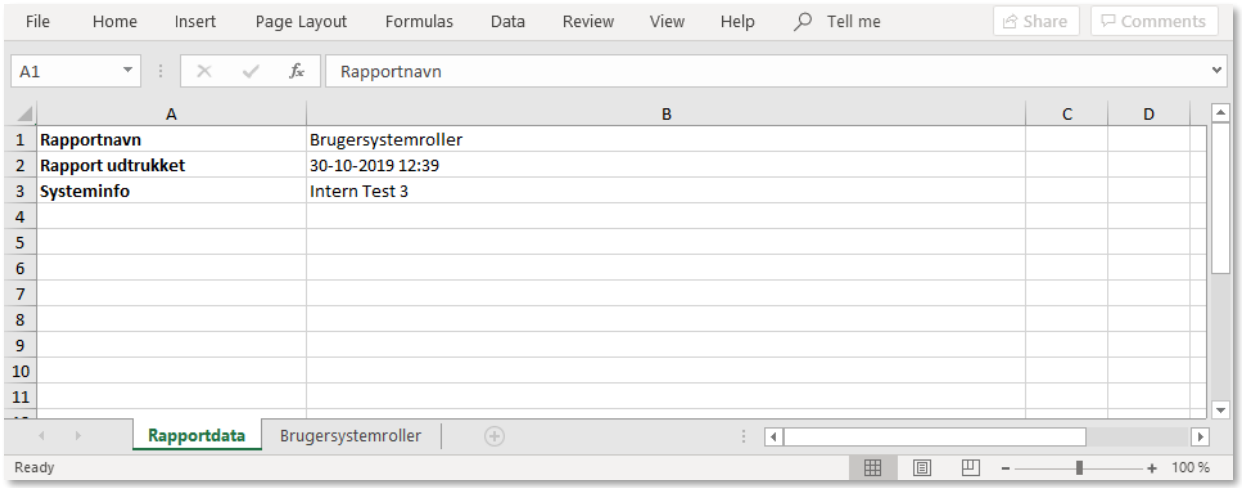


2. Tryk på knappen ”Generer rapport”. Rapporten har filtypen .xlsx.



3. Rapporten modtages i browseren og kan åbnes i Excel direkte, eller ved at gemme den først og herefter åbne den.

4. Rapporten ”Brugersystemroller” indeholder to faneblade i Excel-arket, ”Rapportdata” og ”Brugersystemroller”.



Fanen ”Rapportdata” indeholder følgende informationer:

- Rapportnavn: For denne rapport står der ”Brugersystemroller”
- Rapport udtrukket: Her vises dato og tidspunkt for hvornår rapporten er udtrukket

Systeminfo: Her vises på hvilket miljø, rapporten er udtrukket

Fanen ”Brugersystemroller” indeholder følgende kolonner:

- Leverandør
- Leverandør CVR
- Leverandør UUID
- Brugervendt system
- Brugervendt system UUID
- Brugervendt system EntityId
- Brugersystemrolle
- Brugersystemrolle UUID
- Brugersystemrolle EntityId
- Jobfunktionsrolle
- Jobfunktionsrolle UUID
- Jobfunktionsrolle EntityId
- Dataafgrænsningstype
- Dataafgrænsningstype EntityId

- Dataafgrænsningsværdi
- Dynamisk
- Myndighed
- Myndighed CVR
- Myndighed UUID

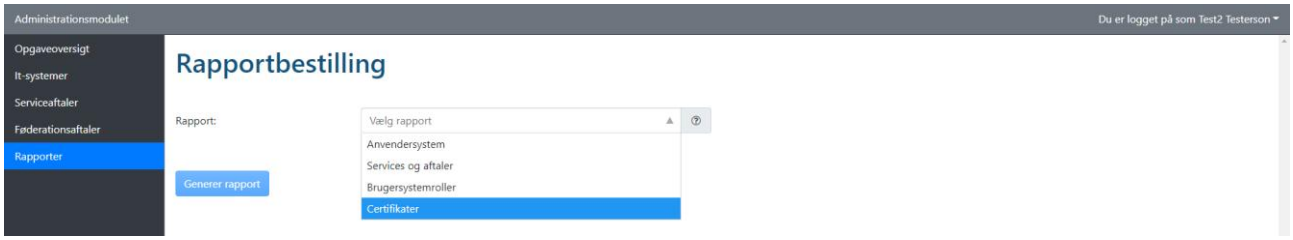
Resultat: Du har fået vist rapporten ”Brugersystemroller - <organisationsnavn> - <miljø>”.

NB: <miljø> angiver hvilket miljø, rapporten er generet fra, Exttest eller Prod. <organisationsnavn> angiver hvilken organisation brugeren, der generer rapporten, repræsenterer.

Rapport: ”Certifikater”. Rapporten viser lister af certifikater for leverandørers anvendersystemer, callback-endpoints eller indeholdt i SAML metadata for brugervendte systemer/Identity Providers.

Vejledning:

5. I Administrationsmodulet skal du vælge punktet Rapporter i venstremenuen. Herefter skal du fra dropdown-listen vælge, hvilken rapport du ønsker at generere, i dette tilfælde skal du vælge ”Certifikater”.

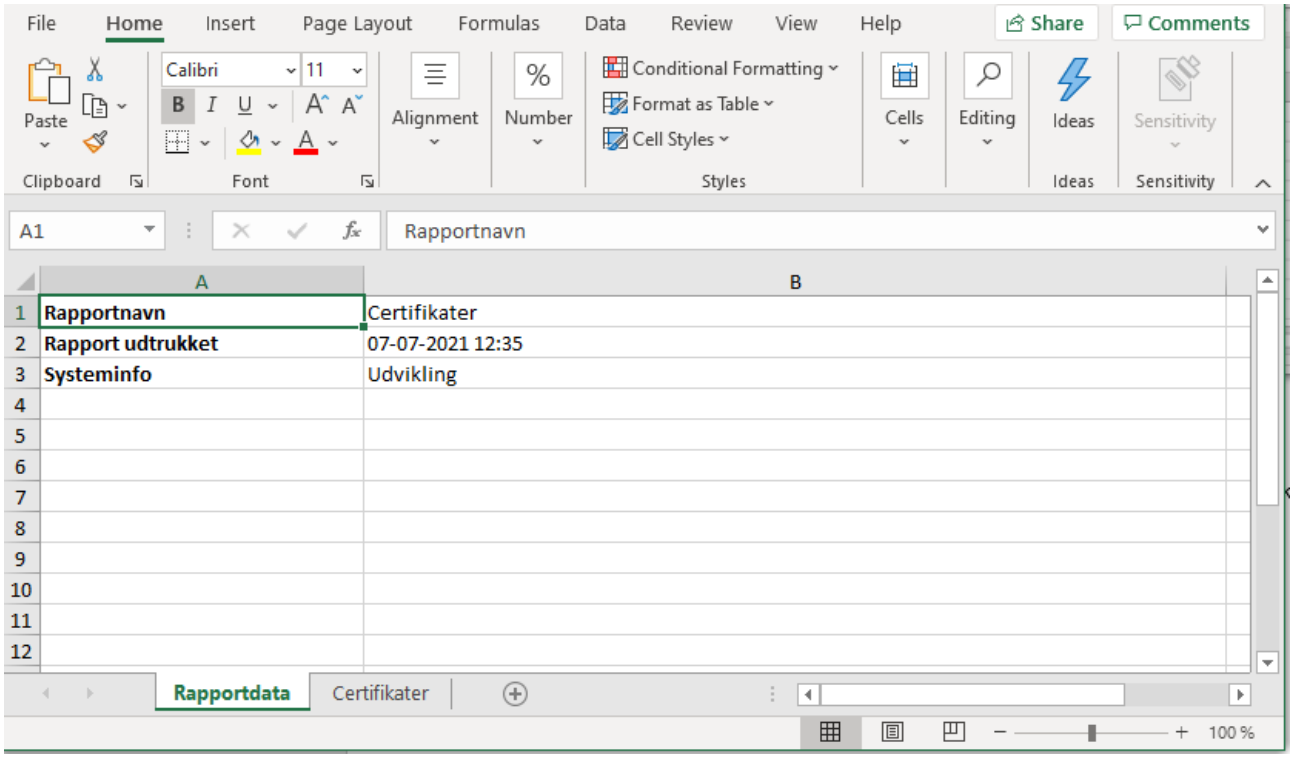


6. Tryk på knappen ”Generer rapport”. Rapporten har filtypen .xlsx.



7. Rapporten modtages i browseren og kan åbnes i Excel direkte, eller ved at gemme den først og herefter åbne den.

8. Rapporten ”Certifikater” indeholder to faneblade i Excel-arket, ”Rapportdata” og ”Certifikater”.



Fanen ”Rapportdata” indeholder følgende informationer:

- Rapportnavn: For denne rapport står der ”Certifikater”
- Rapport udtrukket: Her vises dato og tidspunkt for hvornår rapporten er udtrukket
- Systeminfo: Her vises på hvilket miljø, rapporten er udtrukket

Fanen ”Certifikater” indeholder følgende kolonner:

- Relation
- Navn
- CVR-nr
- It-system (navn)
- It-system (UUID)
- Common Name
- Certifikat CVR
- Certifikat RIF/FID/UID
- Certifikattype
- Certifikatudsteder
- Gyldig fra
- Gyldig til
- Dage til udløb

Resultat: Du har fået vist rapporten ”Certifikat - <organisationsnavn> - <miljø>”.

NB: <miljø> angiver hvilket miljø, rapporten er generet fra, Exttest eller Prod. <organisationsnavn> angiver hvilken organisation brugeren, der generer rapporten, repræsenterer.

Vær også opmærksom på at ”Dage til udløb” er en statisk beregning, og skal derfor relateres til udtræksdato fra ”Rapportdata” fanen.

Certifikattype angiver om der er tale om f.eks. et FOCES-, VOCES- eller OCES3-certifikat.

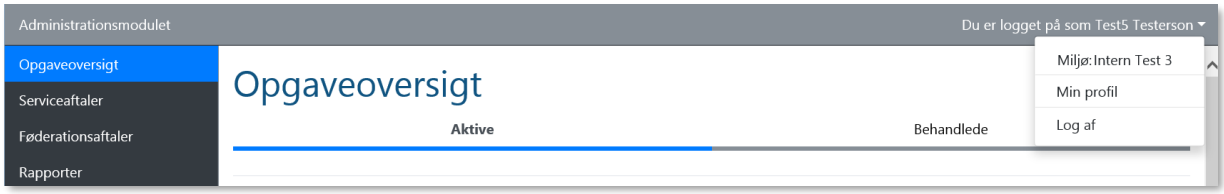
5.23 Brugerprofil

Dette afsnit beskriver to scenarier, dels hvordan man kan se sin egen brugerprofil, og dels hvordan man kan se en oversigt af sin organisations brugerprofiler, hvis man har en rolle, der tillader det.

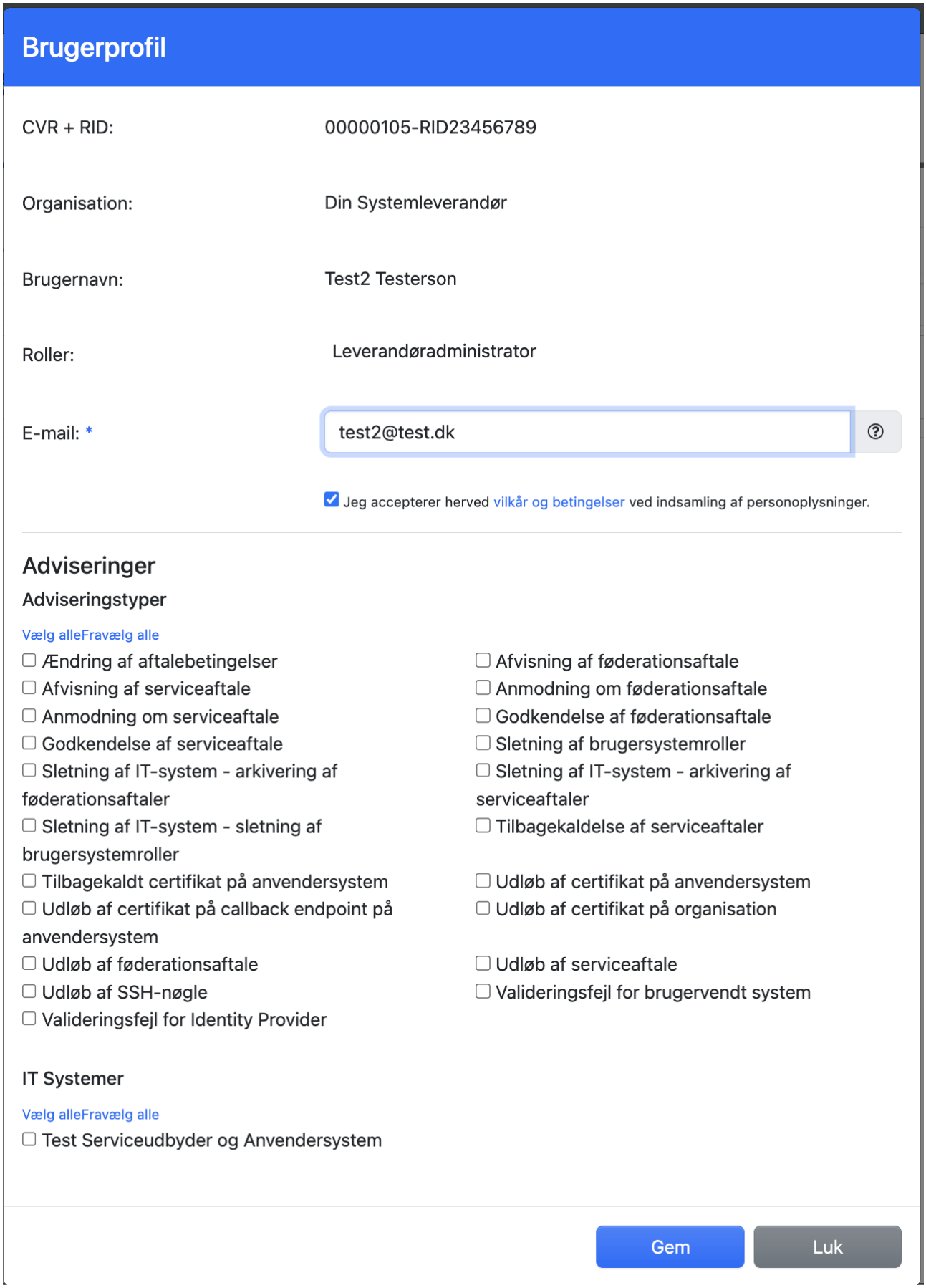
Brugeren: Med rollerne Organisationsadministrator kan du se din brugerprofil.

Vejledning:

1. I Administrationsmodulet skal du i øverste højre hjørne klikke på den lille pil ud for dit navn, hvorefter du skal vælge ”Min profil”.



2. Herefter får du vist din brugerprofil.


Brugerprofil
CVR + RID:
00000105-RID23456789
Organisation:
Din Systemleverandør
Brugernavn:
Test2 Testerson
Roller:
Leverandøradministrator
E-mail: *
test2@test.dk
Jeg accepterer herved vilkår og betingelser ved indsamling af personoplysninger.
Adviseringer
Adviseringstyper
Vælg alleFravælg alle
Ændring af aftalebetingelser
Afvisning af serviceaftale
Anmodning om serviceaftale
Godkendelse af serviceaftale
Sletning af IT-system - arkivering af føderationsaftaler
Sletning af IT-system - sletning af brugersystemroller
Tilbagekaldt certifikat på anvendersystem
Udløb af certifikat på callback endpoint på anvendersystem
Udløb af føderationsaftale
Udløb af SSH-nøgle
Valideringsfejl for Identity Provider
Afvisning af føderationsaftale
Anmodning om føderationsaftale
Godkendelse af føderationsaftale
Sletning af brugersystemroller
Sletning af IT-system - arkivering af serviceaftaler
Tilbagekaldelse af serviceaftaler
Udløb af certifikat på anvendersystem
Udløb af certifikat på organisation
Udløb af serviceaftale
Valideringsfejl for brugervendt system
IT Systemer
Vælg alleFravælg alle
Test Serviceudbyder og Anvendersystem
Gem
Luk

Under din brugerprofil får du vist:

- CVR + RID: Her vises din organisations CVR nr. samt din NemID medarbejdersignaturs unikke ID-nummer
- SAML UUID: En unik identifier for brugeren modtaget fra NemLog-in
- Organisation: Her vises den organisation, som du er tilknyttet
- Brugernavn: Her vises dit navn, som det er indtastet på din profil i NEMLOG-IN
- Rolle: Her vises hvilken/hvilke roller du er tildelt i NEMLOG-IN
- E-mail: Her vises din e-mail. Den e-mailadresse der gemmes her bruges som kontakt e-mailadresse samt til at udsende notifikationer fra Administrationsmodulet, hvis det er relevant i forhold til din rolle.
- Vilkår og betingelser: Her angives at man har accepteret systemets vilkår og betingelser.
- Adviseringer: Her kan der til- og fravælges ønskede adviseringer på både adviseringstype og på IT System. Som default for nye brugere er alt slået til.

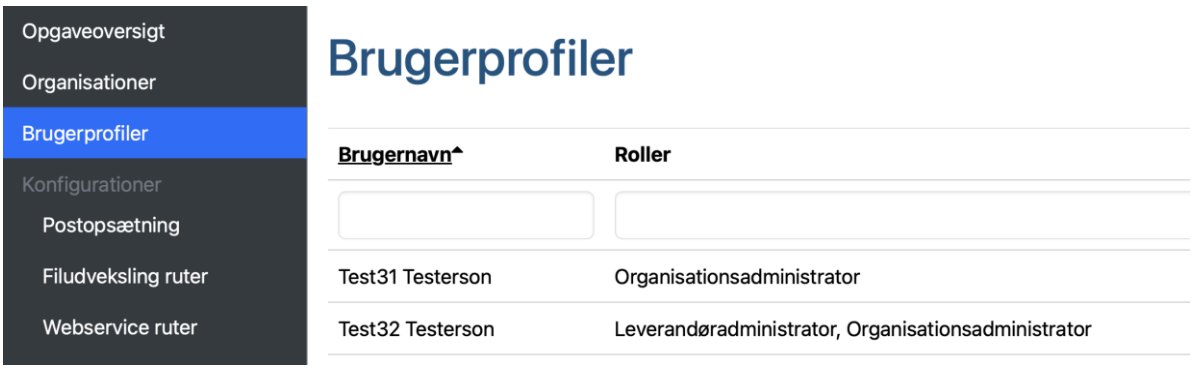
Hvis du vil gemme ændringer, så afslut med at trykke på knappen ”Gem”.

Resultat: Du har fået vist din brugerprofil, og haft mulighed for at redigere din e-mailadresse.

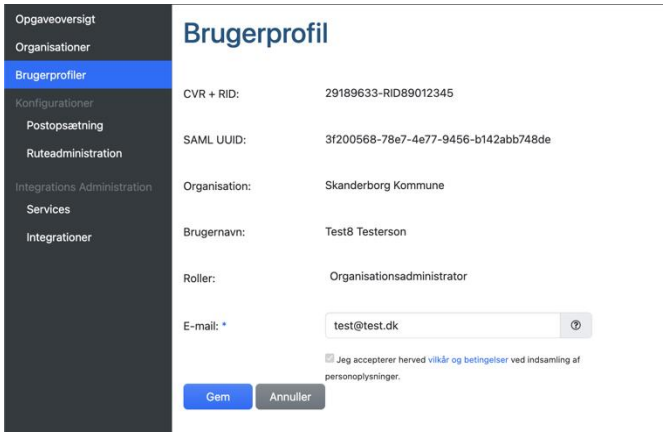
Brugeren: Med rollen Organisationsadministrator kan du udover ovenstående se en liste over organisationens brugere.

Vejledning:

1. I Administrationsmodulet skal du vælge punktet Brugerprofiler i venstremenuen. Herefter får du et overblik over brugerprofiler, som er tilknyttet din organisation. Overblikket viser brugernavn og tilknyttede roller. Du kan fremsøge en brugerprofil ved at søge i feltet Brugernavn. Vælg en brugerprofil fra listen ved at klikke på den.



2. Når du har valgt en brugerprofil, kan du se detaljer for brugerprofilen.



3.

Under de enkelte brugerprofiler får du vist:

- CVR + RID: Her vises din organisations CVR nr. samt din NemID medarbejdersignaturs unikke ID-nummer
- SAML UUID: En unik identifier for brugeren modtaget fra NemLog-in
- Organisation: Her vises den organisation, som du er tilknyttet
- Brugernavn: Her brugerens navn, som det er indtastet på vedkommendes profil i NEMLOG-IN
- Rolle: Her vises hvilken/hvilke roller brugeren er tildelt i NEMLOG-IN. Bemærk at da en brugers roller kun kan synkroniseres mellem NEMLOG-IN og Administrationsmodulet ved, at brugeren logger ind i Administrationsmodulet, kan det ske at rolletildelingen i Administrationsmodulet ikke matcher den konkrete i NEMLOG-IN.
- E-mail: Her vises brugerens e-mail. Den e-mailadresse der gemmes her bruges som kontakt e-mailadresse samt til at udsende notifikationer fra Administrationsmodulet, hvis det er relevant i forhold til brugerens rolle(r).

E-mailadressen er det eneste felt, du kan redigere. Hvis du vil gemme ændringer, så afslut med at trykke på knappen ”Gem”.

Resultat: Du har fået vist de brugerprofiler, der er knyttet til din organisation.

5.24 Adviseringer

Brugeren: Med rollerne Leverandøradministrator og Organisationsadministrator kan du modtage adviseringer.

Administrationsmodulet sender automatisk adviseringer ud for en række hændelser. Det er din rolle, samt adviseringsvalg på brugerprofilen (se under vejledning pkt. 5) der afgør, hvilke adviseringer du modtager.

Som Leverandøradministrator vil du modtage adviseringer på følgende hændelser:

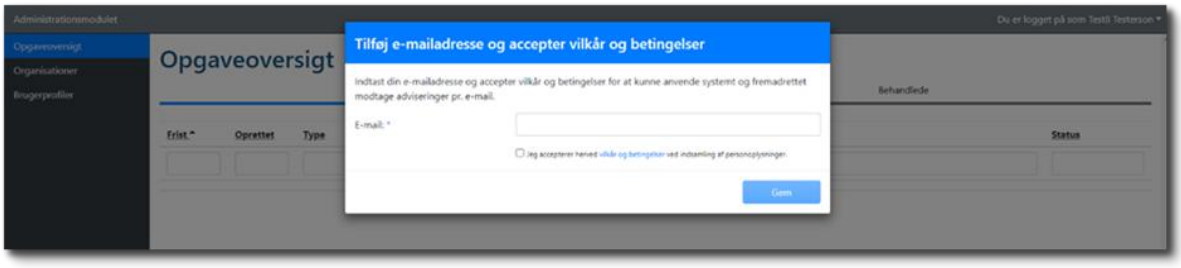
- Afvisning af føderationsaftale: Sendes når en myndighed afviser anmodningen om en føderationsaftale, som din organisation har oprettet.
- Afvisning af serviceaftale: Sendes når en myndighed afviser anmodningen om en serviceaftale, som din organisation har oprettet.
- Godkendelse af føderationsaftale: Sendes når en myndighed godkender en anmodningen om en føderationsaftale, som din organisation har oprettet.
- Godkendelse af serviceaftale: Sendes når en myndighed godkender en anmodningen om en serviceaftale, som din organisation har oprettet. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.
- Udløb af et certifikat tilkoblet en af din organisations anvendersystemer: Sendes 3 måneder før certifikatet udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.
- Udløb af et certifikat indlejret i saml metadataen for en af din organisations brugervendte systemer: Sendes 3 måneder før certifikatet udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.
- Udløb af et certifikat indlejret i saml metadataen for en af din organisations Identity Providere: Sendes 3 måneder før certifikatet udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.
- Udløb af certifikat på en af din organisations serviceaftaler der indeholder en callbackservice: Sendes 3 måneder før certifikatet udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.
- Udløb af en af din organisations føderationsaftaler: Sendes 14 dage før en føderationsaftale udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.
- Udløb af en af din organisations serviceaftaler: Sendes 14 dage før en serviceaftale udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.
- Ændring af aftalebetingelser: Sendes hvis aftalebetingelser opdateres hos KOMBIT.
- Udløb af en SFTP nøgle tilkoblet et af din organisations anvendersystemer: Senest 3 måneder før nøglen udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.

Som Organisationsadministrator vil du modtage adviseringer på:

- Udløb af et certifikat tilkoblet din organisation: Sendes 3 måneder før certifikatet udløber. Dette vil også blive vist på opgaveoversigten, jf. afsnit 5.6.

Vejledning:

1. Første gang du logger ind i Administrationsmodulet vil du automatisk blive spurgt efter at tilføje en e-mailadresse, det er den som vil blive brugt hvis du fremadrettet ønsker at modtage adviseringer pr. e-mail. Systemet vil i samme omgang bede om en kvittering på vilkår og betingelser for brugen af systemet. Hvis linket til "Vilkår og betingelser" bliver valgt, vil disse blive vist. Angiv en e-mail, acceptér betingelserne og afslut med at trykke på knappen "Gem".

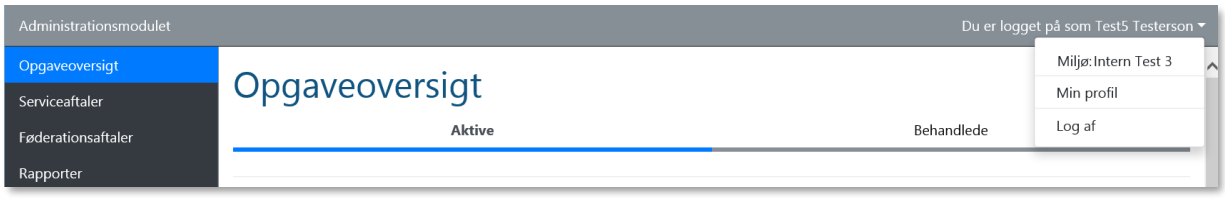


2. Når du har gemt, får du en bekræftelse på skærmen, som vist nedenfor.

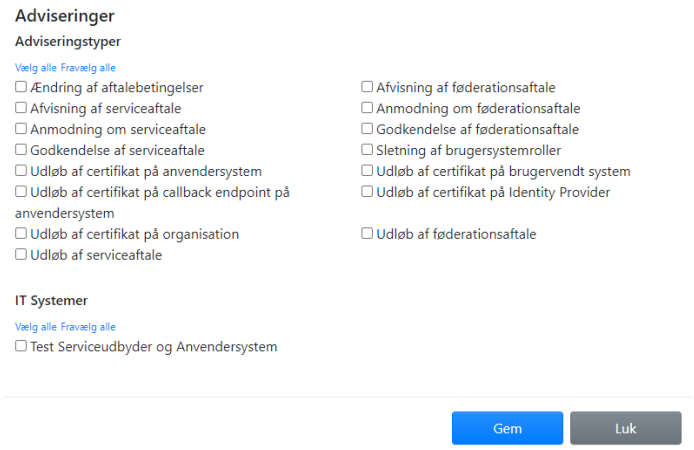


3. Hvis du på et senere tidspunkt, har brug for at ændre din e-mailadresse, kan du gøre det under din brugerprofil. Se punkt 5.23. om brugerprofil.

4. Under menupunktet i øverste højre hjørne vælges min profil.



5. Nu bliver brugerprofilen vist, se 7.14. Nederst på siden er der mulighed for at vælge forskellige adviseringer til og fra. Adviseringer er opdelt i to dele, en for Adviseringstyper og en for It-Systemer. Hvis man f.eks. ønsker at modtage en advisering omkring " Ændring af aftalebetingelser", vælges denne og man vil så få adviseringer omkring dette tilsendt til den e-mailadresse som er angivet på brugerprofilen.



Nogle adviseringstyper knytter sig til et It-System, andre ikke.

Adviseringstyper som anvendes uden IT-System
Ændring af aftalebetingelser
Anmodning om føderationsaftale
Anmodning om serviceaftale
Sletning af brugersystemroller
Sletning af IT-system - arkivering af føderationsaftaler
Sletning af IT-system - arkivering af serviceaftaler
Sletning af IT-system - sletning af brugersystemroller
Udløb af certifikat på organisation
Udløb af føderationsaftale
Udløb af serviceaftale

Adviseringstyper som anvendes med et IT-System	
Adviseringstyper	*IT-system kontekst*
Afvisning af føderationsaftale	Identity provider
Afvisning af serviceaftale	Anvendersystem
Godkendelse af føderationsaftale	Identity provider
Godkendelse af serviceaftale	Anvendersystem

Udløb af certifikat på anvendersystem	Anvendersystem
Udløb af certifikat på brugervendt system	Brugervendt system
Udløb af certifikat på callback endpoint på anvendersystem	Anvendersystem
Udløb af certifikat på Identity Provider	Identity provider

Resultat: Du har tilføjet din e-mailadresse, samt ønskede adviseringer og vil fremadrettet modtage adviseringer for disse, på den angivne e-mail.

6 Testmuligheder som Myndighed

Til testformål har du som leverandør mulighed for at blive ændret til rollen "Myndighed", da det giver en række muligheder for at teste funktionaliteten i den fælleskommunale infrastruktur, inden du involverer en kommune i din test.

Denne mulighed er særlig relevant for dig der:

- skal teste STS Organisation og gerne vil gøre det med din egen testdata, inden du tester med en aftalt kommunes testdata.

- anvender KOMBITs adgangstyring for brugere, da det giver dig mulighed for at afprøve dit systems implementering af sikkerhedsmodellen samt håndhævelse af de brugersystemroller dit system udstiller.

- anvender adgangsstyring for systemer, dvs skal trække tokens fra Security Token Service til enten demoservice-clienten eller en anden integration.
  Du kan også agererer serviceudbyder og udstille services via STS Administration, så du kan verificere kvaliteten af den service, du udbyder, før du tillader andre at anvende din service.

BEMÆRK! *Du kan altså* ***kun*** *teste med dig selv som myndighed for følgende integrationer/områder:*

- *STS Organisation*
- *Adgangsstyring for brugere*
- *Adgangsstyring for systemer*

Du skal derfor ikke forsøge at teste med andre services som fx CPR, Print, Beskedfordeleren og indeksene. Det er ikke sikkert, at det vil virke, og du skal derfor ikke forvente support og hjælp til fejlsøgning for disse integrationer, hvis du benytter dig selv som myndighed. Hvis du skal teste med disse integrationer, skal du have en aftale med en kommune.

6.1 Test med støttesystemet Organisation

Har du behov for at teste støttesystemet Organisation med dine egne organisationsdata, skal du kontakte FKI@kombit.dk , for at få oprettet de nødvendige konfigurationer i STS Organisation, Serviceplatformen samt STS Administration, før du kan påbegynde din test.

6.2 Test af adgangsstyring for brugere

Når du som leverandør har fået rollen Myndighed, har du mulighed for at afprøve din implementering af adgangsstyring for brugere med dig selv som myndighed, før du involerer en konkret kommune i din test.

Som myndighed kan du oprette din egen Identity Provider og indgå føderationsaftale til din egen myndighed, samt oprette jobfunktionroller til de brugere, du ønsker at teste med.

Når du opretter dit brugervendte it-system skal du huske at afgrænse til dig selv som myndighed, så andre ikke kan begynde at anvende de brugersystemroller du udbyder.

Når du skal teste med rigtige kommuner, skal du udvide afgrænsningen til at omfatte de releavnte kommuner. Du kan læse mere om, hvordan du opretter og redigerer myndighedsafgrænsninger i afsnit 5.6.

6.3 Test af adgangsstyring for systemer

Første gang du skal trække tokens fra Security Token Service, kan du øve dig ved at benytte demoservice-clienten udstillet på GitHub – læs eventuel mere i Programmers Guide til Sikkerhed i den Fælleskommunale Infrastruktur.

Når du som leverandør har fået rollen myndighed, skal du godkende serviceaftaler på dine egne vegne. Din organisation vil fremgå af listen af myndigheder alle kan vælge at indgå en serviceaftale med, hvilket betyder du også kan modtage serviceaftale anmodninger fra andre end dig selv.

Indgår du en serviceaftale hvor du er myndigheden, skal du være opmærksom på, at ikke alle services er udbudt i infrastrukturen (der hvor det ikke er relevant at teste med dig selv som myndighed). Nogle services kan også være helt afgrænset for test med andre end rigtige myndigheder.

Udbyder du en service via STS Administration anbefaler vi, at du selv tester din implementering i sammenhæng med Adgangsstyring for systemer (Security Token Service), før du giver andre mulighed for at tilgå din service(s).

Mens du tester og verificerer at din service har den forventede kvalitet, skal du huske at lægge en myndighedsbegrænsning på, som kun giver dig selv som myndighed adgang til at indgå serviceaftaler på din service, ellers vil andre kunne begynde at teste mod din service, før du ønsker det.

Når du er færdig med testen, skal du fjerne myndighedsbegrænsningen så de myndigheder du ønsker at udbyde din service til, kan indgå serviceaftaler på den.

6.4 Sådan bliver du myndighed i testmiljøet

Sådan får du som leverandør rollen Myndighed i testmiljøet:

1. Bestil ydelsen ”Oprettelse af som Egen Test Myndighed – Grundpakken” i Digitaliseringskataloget.
2. Når ydelsen er bestilt, modtager du et bestillingsID, som du skal notere i bestillingsblanketten, du finder nederst på siden i linket ovenfor.
3. På blanketten skal du bl.a oplyse hvilket rolledomæne[1], du ønsker tilknyttet dig som myndighed, og samtidig skal du godkende vilkårene for at være myndighed i testmiljøet.
4. Send den udfyldte og underskrevne blanket til helpdesk@serviceplatformen.dk. Når bestillingen er behandlet, modtager du bekræftelse fra Helpdesk på, at din organisation nu er registreret som myndighed i testmiljøet.
5. Få din Nemlog-In Administrator til at tildele dig de myndighedsroller, du har brug for:

[1] Rolledomænet anvendes på samtlige af organisationens jobfunktionsroller. Et rolledomæne kan fx være: "kombit.dk". Rolledomænet skal bestå af mindst to led adskilt med punktum, hvert led skal bestå af mindst to tegn, hvor tilladte tegn er a-z, A-Z, 0-9 samt bindestreg og underscore, dog må første tegn i et led ikke være bindestreg eller underscore.

-
    - For at godkende serviceaftaler og føderationsaftaler skal du have rollen: **Aftaleadministrator (test)**
    - For at oprette jobfunktionsroller til dine brugere skal du have rollen: **Rolleadministrator (test)**
    - Du kan finde mere hjælp til rolletildeling i Vejledning til NemLogin.

6.5 Vilkår for leverandører der agerer myndighed i testmiljøet

Før din organisation kan få tildelt rollen mynighed i testmiljøet, skal du acceptere nedenstående vilkår:

- Myndighedsrollen tildeles kun i testmiljøet til leverandører.
- Når du agerer myndighed i testmiljøet, har du ansvar for de data der er lagt i Støttesystemerne. Du må som myndighed ikke godkende serviceaftaler med andre leverandører end dig selv. Hvis du modtager en serviceaftaleanmodning fra en anden leverandør, skal du afvise den.
- Du må **aldrig** anvende eller indlæse produktionsdata i testmiljøet.
- Du er forpligtet til at orientere øvrige anvendere af den fælleskommunale infrastruktur i din organisation, om de ovenstående vilkår.

7 Kontakt og Support

Er der spørgsmål eller behov for yderligere afklaringer, kan der tages kontakt til Serviceplatformens Helpdesk på helpdesk@serviceplatformen.dk eller tlf.: 70 11 15 39.