

DIGITALISERINGSSTYRELSEN



Brugermanual til NemLog-in administration

Til Teknisk administrator, Administrator for it-systemudbyder og Administrator for it -
leverandør

Contents

Changelog.....	4
1 Introduktion	5
2 Tilsluttede aktører.....	6
2.1 NemLog-in support	6
2.2 Tjenesteudbyder.....	6
2.3 It-leverandør	6
2.4 Brugerorganisationer	6
3 Brugerroller.....	7
3.1 NemLog-in administrator	7
3.2 Administrator for it-systemudbyder	7
3.3 Teknisk administrator	7
3.4 Administrator for it-leverandør	8
4 Opgaver.....	9
4.1 Tilslut nyt it-system uden privilegier til log-in-tjenesten (SSO)	9
4.2 Tilslut nyt it-system til signeringstjenesten.....	10
4.3 Tilslut nyt it-system der indeholder privilegier til log-in-tjenesten	12
4.4 Tilslut ny Web Service Provider til STS	14
4.5 Tilslut nyt it-system til log-in-tjenesten (SSO) der indeholder fuldmagtsprivilegier rettet mod borgere 18	
4.6 Opdater eksisterende tilslutning til log-in-tjenesten (herunder certifikatudskiftning)	21
4.7 Oprettelse af Lokal STS – Local Token Case	23
4.8 Opdatering af metadata for anvendelse af STS – Bootstrap Token Case.....	23
4.9 Registrering i CSS – Signature Case.....	23
4.10 Oprette og vedligeholde tekniske data for en systembruger	23
5 Ventende opgaver.....	25
5.1 Se ventende opgaver	25
5.2 Håndtér en opgave.....	26
5.3 Opgaver til administrator for it-systemudbyder	27
6 Håndtering af it-systemer.....	28
6.1 Se oversigt over it-systemer	28
6.2 Se detaljer for it-system	29
6.3 Opdater oplysninger om it-system	31
6.4 Opret nyt it-system	32
6.5 Tilføj en teknisk administrator.....	34
6.6 Fjern en teknisk administrator.....	36
6.7 Slet it-system	37

6.8	Tilføj en it-leverandør	38
6.9	Fjern en it-leverandør	39
7	Teknisk tilslutning af it-system.....	40
7.1	Se it-systemets tekniske data	40
7.2	Rediger tekniske oplysninger om it-systemet	43
7.3	Administrer adgang til fuldmagtstjeneste	45
7.4	Tilføj et nyt privilegie	46
7.5	Opdatér privilegie	48
7.6	Fjern privilegie	49
7.7	Indlæs tekniske data (metadatafil).....	50
7.8	Download NemLog-in metadata	51
7.9	Validér tekniske data (metadata).....	52
7.10	Se versioner af teknisk data (metadata) – kun produktion	53
7.11	Opret en ny version af teknisk data (metadata).....	54
7.12	Tilføj en NemID borgertestbruger	55
7.13	Tilføj en MitID borgertestbruger.....	58
7.14	Tilføj en NemID medarbejdertestbruger	60
7.15	Tilføj en MitID medarbejdertestbruger.....	62
7.16	Opdatér privilegier for eksisterende borgertestbruger	64
7.17	Opdatér eksisterende medarbejdertestbruger.....	64
7.18	Fjern en testbruger	65
7.19	Indlæs testrapport	66
7.20	Download testrapport	67
7.21	Ansøg om integrationstest	68
7.22	Anmod om overførsel til produktion	69
7.23	Skift Certifikat	70
7.24	Opret ny systembruger	71
7.25	Vedligehold systembruger.....	72
7.26	Provisioner systembruger til integrationstest.....	73
7.27	Provisioner systembruger til Produktion	74
7.28	Skift System Bruger Ejer	74
7.29	Anmod om web service adgang.....	75
7.30	Supporter systembruger	76
7.31	Godkend eller afvis systembrugeranmodning til webtjeneste	76
7.32	Tildel og fjern system privileger til systembrugere	77
7.33	Tilføj test systembruger	79
8	Drift Status.....	81

Changelog

Date	Version	Change description	Initials
2015-05-08	0a	Nyt dokument	
2015-05-19	1.4	Publiceret version	
2017-09-07	2	Layout opdateret Opdatering til afsnit 4.5, 7.1, 7.2 vedr. ny metadata attribut og målgruppe ifbm. udrulning af NemID Privat til Erhverv.	
2020-01-11	3.0	Afsnit 12, 13, 16 og 17 vedr. testbrugere opdateret/tilføjet. Links til specifikke sider rettet igennem hele dokumentet.	Søren C. Bauer
2021-05-25	3.1	Omlagt til nyt design	SPEDE
2021-08-30	3.2	Fejl rettet på forside, mgl. krydsreferencer tilføjet, konsekvensrettet til "it" med småt. Link til https://tu.nemlog-in.dk/testrapport/ afløser link til testrapport på digitaliser.dk Markering af roller i brødteksten fjernet.	SPEDE

Update the footer w. date, version and initials as well.

1 Introduktion

Denne manual beskriver brugen af administrationsmodulet til NemLog-in, der findes på <https://administration.nemlog-in.dk>. Den henvender sig til tjenesteudbydere og it-leverandører, som skal udføre opgaver i forhold til tilslutning samt administration af it-systemer i NemLog-in.

Du kan yderligere finde hjælp til NemLog-in support på Digitaliser.dk <http://digitaliser.dk/group/2550185>

Opgaver i administrationsportalen, der er henvendt til brugerorganisationer og support er ikke inkluderet i denne brugermanual.

2 Tilsluttede aktører

2.1 NemLog-in support

Digitaliseringsstyrelsen står for support i forhold til tilslutning og vedligeholdelse af it-systemer i administrationsmodulet.

Erhvervsstyrelsen står for support af alle brugerorganisationer som ikke har indgået en supportaftale, der har behov for at benytte brugeradministration og MitID Erhverv.

2.2 Tjenesteudbydere

Tjenesteudbydere kaldes i NemLog-in/Administrationen for en it-systemudbyder. Det er en myndighed eller en privat virksomhed, der stiller et it-system til rådighed for borgere, virksomheder eller andre offentlige myndigheder. It-systemudbyderen er ansvarlig for it-systemet, herunder tilslutning til NemLog-in. Dette indebærer, at it-systemudbyderen skal underskrive nærværende vilkår og påtage sig ansvaret for it-systemet.

En privat virksomhed, i rollen som it-systemudbyder eller broker, kan ikke bruge log-in servicen (SSO), det kan kun offentlige myndigheder.

I NemLog-in/Administrationen kan en it-systemudbyder også være en gateway-leverandør. I det tilfælde er it-systemudbyder en it-leverandør eller myndighed, hvis systemmæssige tilslutning til NemLog-in anvendes til at betjene flere offentlige myndigheder. Dette kan eksempelvis være en fælleskommunalløsning, der leveres af en it-leverandør, eller et antal kommuner, der indgår i et driftsfællesskab. Bemærk at rollen som gateway-leverandør udgår og bliver erstattet af NemLog-in broker konstruktionen.

2.3 It-leverandør

It-leverandør er en leverandør, der har indgået kontrakt med en offentlig myndighed om levering af et it-system, hvor myndigheden har rollen som it-systemudbyder.

2.4 Brugerorganisationer

Alle organisationer der skal benytte brugerrettigheder igennem en NemLog-in løsning, skal være oprettet i NemLog-in. Brugerorganisationer administrerer deres organisation og rettigheder i <https://brugeradministration.nemlog-in.dk>.

Menupunktet *Brugeradministration* kan forekomme i administrationsmodulet, men da denne funktionalitet ikke er relevant i forhold til administration af it-systemer, er tilknyttede roller og funktionalitet ikke medtaget i denne manual. Der kan på virk.dk finde guides vejledning og support til hvordan brugeradministrationen benyttes.

3 Brugerroller

Når du tilgår administrationsportalen, vil systemet identificere dig på baggrund af dit login. Menuen du ser, afhænger derfor af de roller, der er tilknyttet til dit medarbejdercertifikat. Følgende roller er aktuelle i forhold til administration af it-systemer.

I NemLog-in supporten benyttes følgende roller til at administrere tilslutning af it-systemer:

- NemLog-in administrator

Hos tjenesteudbydere benyttes følgende roller til administration af it-systemer:

- Administrator for it-systemudbyder
- Teknisk administrator (kun relevant i tilfælde, hvor tjenesteudbydere administrerer deres egen tilslutning eller agerer som gateway-leverandør)

Hos it-leverandørerne er der følgende roller:

- Administrator for it-leverandør
- Teknisk administrator

3.1 NemLog-in administrator

Rollen administreres af Digitaliseringsstyrelsen og anvendes i forhold til support af offentlige tjenesteudbydere og it-leverandører. Herunder oprettelse af rettigheder og fuldmagtspakker i brugeradministrationen, samt godkendelse af opgaver i forbindelse med tilslutning og administration af it-systemer.

3.2 Administrator for it-systemudbyder

Administratoren for it-systemudbyderen har til opgave at oprette nye tilslutninger af systemer i NemLog-in for tjenesteudbyderen. Administratoren skal også godkende, at første version af et system kan overføres til integrationstest, samt godkende at den nye version af systemet kan overføres til produktion.

Den tekniske administration af it-systemerne overlades til den tekniske administrator (se afsnit 3.3). Udnævn derfor en eller flere tekniske administratorer, hvis jeres organisation selv ønsker at administrere systemet eller tilføje en it-leverandør til et specifikt system, hvis organisationen ikke selv skal administrere deres system.

3.3 Teknisk administrator

Den tekniske administrator registrerer og vedligeholder teknisk information om et it-system. Rollen kan enten tildeles internt hos it-systemudbyderen eller uddelegeres til en it-leverandør, som ofte er en privat virksomhed.

Den tekniske administrator vedligeholder teknisk metadata omkring et it-system, såsom end-points, certifikater, privilegier, attributter, SAML-metadata (i tilfælde af web applikationer) og systemstatus (test og produktion).

Det er derfor den tekniske administrator, som har ansvar for hovedparten af opgaverne i forbindelse med tilslutningen af et it-system, og denne person kan oprette nye versioner af et system og anmode om, at systemet bliver overført til integrationstest eller produktion.

3.4 Administrator for it-leverandør

Tjenesteudbydere vil ofte indgå aftale med en it-leverandør om at udvikle, hoste og vedligeholde en række af deres it-løsninger. Administratoren for it-leverandøren skal udpege en eller flere tekniske administratorer til en løsning, som it-leverandøren skal administrere for en tjenesteudbyder, det der i systemet kaldes en it-systemudbyder.

4 Opgaver

Dette kapitel indeholder flows for typiske opgaver, der udføres i NemLog-in Administration. Afsnittet beskriver ikke detaljeret, hvordan de enkelte handlinger foretages, men henviser til hvem der typisk skal udføre en handling, og hvor handlingen er beskrevet mere detaljeret i denne brugermanual.

4.1 Tilslut nyt it-system uden privilegier til log-in-tjenesten (SSO)

Dette flow beskriver hvilke opgaver, der skal udføres i forbindelse med oprettelsen af et it-system, der benytter log-in-tjenesten (SSO) - men som ikke skal benytte OIOSAML-privilegieattributen eller trækker data fra NemLog-in Brugeradministration.

For at tilslutte et nyt it-system, skal Administrator for it-systemudbyder være logget ind i NemLog-in Administrationen:

4.1.1 "Opret nyt it-system" (beskrevet i afsnit 6.4).

Her skal Log-in-tjenesten (SSO) vælges - Signeringstjeneste kan også vælges i samme tilslutning. Det nyoprettede it-system vil nu få status Påbegyndt.

Hvis det nyoprettede system, skal håndteres af en it-leverandør, skal Administratoren for it-systemudbyderen tilføje denne:

4.1.1.1 "Tilføj en it-leverandør" (beskrevet i afsnit 6.8).

Administrator for it-leverandør skal nu udpege en eller flere tekniske administratorer. Hvis tjenesteudbyderen vil administrere deres egen tilslutning, er det i stedet **Administrator for it-systemudbyder**, der skal tilføje denne:

4.1.2 "Tilføj en teknisk administrator" (beskrevet i afsnit 6.5).

Administrator for it-systemudbyder og Administrator for it-leverandør kan se og fjerne tekniske administratorer efter behov. Teknisk administrator skal herefter sørge for, at de tekniske detaljer angående it-systemet bliver klargjort til integrationstest:

4.1.3 "Indlæs tekniske data (metadata-fil)" (beskrevet i afsnit 7.7).

Under indlæsning af metadata vil der foregå en automatisk validering af den uploadede XML-fil. Data skal indeholde et unikt system- eller organisations-testcertifikat, der ikke benyttes af andre NemLog-in tilslutninger, og data skal kunne valideres i forhold til OIOSAML-standard. Teknisk administrator har også mulighed for at validere metadata fra den officielle testportal <https://test-nemlog-in.dk/testportal/> igennem metadatavalidatoren - inden tilslutningen startes i NemLog-in Administrationen.

OBS: Skal systemet anvendes i forbindelse med STS - Bootstrap Token Case scenariet, se da afsnit 4.8.

Teknisk administrator skal nu tage stilling til it-systemets tekniske detaljer, der ikke automatisk blev opdateret ved indlæsning af metadata. Her skal der tilføjes tidspunkt for, hvornår tilslutning for it-systemet skal være aktivt i integrationstestmiljøet. Målgruppe som systemet er rettet imod skal også defineres, da det har indflydelse på senere validering af metadata. Det udføres gennem følgende opgave:

4.1.4 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2).

Husk at trykke *Gem tekniske oplysninger*, så ændringer foretages.

Teknisk administrator kan nu ansøge om at få systemet i integrationstest. Bemærk, at det ikke vil være muligt at opdatere tekniske detaljer om systemet igen, før integrationstesten er enten godkendt eller afvist. Det unikke entityID vil desuden blive fastlåst for den specifikke tilslutning, så snart der er ansøgt om

integrationstest, og det vil ikke længere kunne ændres for denne tilslutning. For at komme i integrationstest, skal der ansøges herom:

4.1.5 "Ansøg om integrationstest" (beskrevet i afsnit 7.21).

Efter der er anmodet om integrationstest, vil status af systemet være i *Integration test (klar)*, hvorefter it-system og testdata bliver overført til integrationstestmiljøet. Data vil nu være tilgængelige i integrationstest.

It-leverandøren eller Tjenesteudbyderen skal nu udføre integrationstesten i overensstemmelse med de prædefinerede testcases. Vejledning til testcases og skabelon for testrapport findes her: <https://tu.nemlog-in.dk/testrapport/>.

Når testen er gennemført succesfuldt, skal Teknisk administrator uploade en underskrevet testrapport:

4.1.6 "Indlæs testrapport" (beskrevet i afsnit 7.19).

Det er vigtigt at kontrollere, at testrapporten er udfyldt korrekt og uploadet før næste opgave udføres.

Når Testrapport er indlæst korrekt, skal Teknisk administrator godkende, at integrationstesten er afsluttet. Det gøres ved at godkende den opgave, der ligger under fanebladet *Ventende opgaver*.

4.1.7 "Håndtér en opgave" (beskrevet i afsnit 5.2).

NemLog-in supporten modtager nu den udfyldte testrapport og vil nu verificere, at rapporten er fyldestgørende og tage stilling til, om den kan godkendes. Hvis den bliver afvist af NemLog-in supporten, vil systemet igen føres tilbage til status *påbegyndt*, hvorefter tidligere trin skal gentages. Hvis den bliver godkendt, bliver status sat til *Integration test (gennemført)*.

Systemet er nu snart klar til at blive forberedt på produktion. Dette gør Teknisk administrator ved at vælge fanen 'Produktion' og uploade nye metadata, der indeholder produktionscertifikatet:

4.1.8 "Indlæs tekniske data (metadatafil)" (beskrevet i afsnit 7.7).

Dernæst skal produktionstidspunktet angives for, hvornår metadata slår igennem i produktionsmiljøet. Det gør Teknisk administrator ved at opdatere de tekniske data:

4.1.9 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2).

Det er her muligt at indlæse produktionscertifikaterne, hvis de ikke blev uploadet med ny metadata. Efter alle tekniske detaljer er opdateret, kan Teknisk administrator nu anmode om, at systemet går i produktion:

4.1.10 "Anmod om overførsel til produktion" (beskrevet i afsnit 7.22).

Status på systemet vil nu ændre sig til *Produktion (ansøgt)*.

Herefter skal Administrator for it-systemudbyder godkende, at it-systemet går i produktion. Det gøres fra ventende opgaver:

4.1.11 "Håndtér en opgave" (beskrevet i afsnit 5.2).

Når opgaven er godkendt af tjenesteudbyderen vil status på systemet være *Produktion (godkendt)*, hvorefter systemet bliver overført til produktion med status *Produktion (klar)*. Systemet er først aktivt på det angivne tidspunkt for produktion. I tilfælde af, at produktionstidspunkt ligger før den endelige godkendelse, kan der gå op til 5 minutter, før systemet vil fungere.

4.2 Tilslut nyt it-system til signeringstjenesten

Dette flow beskriver hvilke opgaver, der skal udføres i forbindelse med oprettelsen af

et it-system, der kun skal benytte NemLog-ins signeringskomponent. Tilslutningen vil ikke kunne benytte NemLog-ins log-inkomponent.

Bemærk at der nu er to signeringstjenester, betegnet hhv. Signeringstjeneste (legacy) og Kvalificeret signeringstjeneste.

For at tilslutte et nyt it-system skal Administrator for it-systemudbyder logge ind i administrationsportalen og oprette systemet, herunder vælge hvilken af signeringstjenesterne, der skal tilsluttes.

4.2.1 "Opret nyt it-system" (uddyb i afsnit 6.4).

Det er systemtypen Signeringstjeneste (legacy) eller Kvalificeret signeringstjeneste, der skal vælges.

Hvis det nyoprettede it-system skal håndteres af en it-leverandør, skal Administrator for it-systemudbyder tilføje denne:

4.2.1.1 "Tilføj en it-leverandør" (beskrevet i afsnit 6.8).

Herefter skal Administrator for it-leverandør udpege en eller flere tekniske administratorer. Hvis it-systemudbyder vil administrere deres egen tilslutning, er det i stedet Administrator for it-systemudbyder, der skal tilføje en Teknisk administrator:

4.2.2 "Tilføj en Teknisk administrator" (beskrevet i afsnit 6.5).

Administrator for it-systemudbyder og Administrator for it-leverandør kan se og fjerne tekniske administratorer efter behov.

Teknisk administrator skal nu tage stilling til it-systemets tekniske detaljer. Da en ren tilslutning til signeringstjenesten ikke indeholder metadata, skal entityID samt base64 encoded signeringscertifikat tilføjes manuelt. Der skal tilføjes et unikt system- eller organisations-testcertifikat. Endeligt skal der angives et tidspunkt for, hvornår tilslutning for it-system skal være aktivt i integrationstestmiljøet. Det gøres ved at opdatere teknisk data:

4.2.3 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2).

Husk at trykke *Gem tekniske oplysninger*, så ændringer foretages.

Teknisk administrator kan nu ansøge om at få systemet i integrationstest.

Bemærk, at det ikke er muligt at opdatere tekniske detaljer om systemet igen, før integrationstesten er enten godkendt eller afvist. Det unikke entityID bliver desuden fastlåst for den specifikke tilslutning, når der er ansøgt om integrationstest, og der kan ikke længere ændres for tilslutningen. For at komme i integrationstest skal der ansøges herom:

4.2.4 "Ansøg om integrationstest" (beskrevet i afsnit 7.21).

Efter der er anmodet om integrationstest, vil status af systemet være i Integration test (klar), hvorefter system og testdata bliver overført til integrationstestmiljøet. Data vil nu være tilgængelig i integrationstest it-leverandør eller it-systemudbyder skal nu udføre integrationstesten i overensstemmelse med de prædefinerede testcases. Vejledning til testcases og skabelon til testrapport findes her: <https://tu.nemlog-in.dk/testrapport/>. Når testen er gennemført succesfuldt, skal Teknisk administrator uploade en underskrevet testrapport:

4.2.5 "Indlæs testrapport" (beskrevet i afsnit 7.19).

Det er vigtigt at kontrollere, at testrapporten er uploadet og udfyldt korrekt før næste opgave udføres. Når testrapporten er indlæst korrekt, skal Teknisk administrator godkende, at integrationstesten er afsluttet. Dette gøres ved at godkende den opgave, der ligger under ventende opgaver:

4.2.6 "Håndtér en opgave" (beskrevet i afsnit 5.2).

NemLog-in supporten skal nu verificere, at testrapporten er fyldestgørende og tage stilling til, om den kan godkendes. Hvis den bliver afvist af NemLog-in supporten, vil systemet igen føres tilbage til status *påbegyndt*, hvorefter tidligere trin skal gentages. Ved godkendelse af integrationstest, vil status blive sat til *Integration test (gennemført)*.

4.2.7 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2).

Der er her muligt at indlæse produktionscertifikaterne, hvis de ikke blev uploadet med ny metadata. Efter alle tekniske detaljer er opdateret, kan Teknisk administrator anmode om, at systemet går i produktion:

4.2.8 "Anmod om overførsel til produktion" (beskrevet i afsnit 7.22).

Status på systemet vil nu ændre sig til Produktion (ansøgt). Herefter skal Administrator for it-systemudbyderen godkende, at it-systemet går i produktion. Det gøres fra ventende opgaver:

4.2.9 "Håndtér en opgave" (beskrevet i afsnit 5.2).

Når opgaven er godkendt af løsningens it-systemudbyder, vil status på systemet være Produktion (godkendt).

Herefter vil systemet blive overført til produktion med status Produktion (klar). Systemet vil først være aktivt på det angivne produktionstidspunkt.

I tilfælde af, at produktionstidspunktet ligger før den endelige godkendelse, kan der gå op til 5 minutter før systemet vil fungere. Hvis det angivne produktionstidspunkt ligger efter den endelige godkendelse, vil systemet fungere på det angivne tidspunkt.

4.3 Tilslut nyt it-system der indeholder privilegier til log-in-tjenesten

En tilslutning til log-in-tjenesten (SSO) der skal indeholde privilegier, der er tilgængelige igennem NemLog-in Brugeradministration, skal indeholde OIOSAML privilegie attributten. Disse privilegier skal oprettes i NemLog-in Administrationen, som beskrevet i dette flow.

For at tilslutte et nyt it-system skal Administrator for it-systemudbyder logge ind i Administrationen (administration.nemlog-in.dk). For at oprette et nyt it-system skal administratoren først foretage følgende:

4.3.1 "Opret nyt it-system" (beskrevet i afsnit 6.4)

Vælg systemtypen Log-in Service (SSO)- Signeringstjeneste kan også til vælges i samme tilslutning.

Det nyoprettede system vil nu få status Påbegyndt. Hvis systemet skal håndteres af en it-leverandør, skal Administrator for it-systemudbyder tilføje følgende:

4.3.1.1 "Tilføj en it-leverandør" (beskrevet i afsnit 6.8).

Herefter skal Administrator for it-leverandør udpege en eller flere tekniske administratorer. Hvis tjenesteudbyderen vil administrere deres egen tilslutning, er det i stedet Administrator for it-systemudbyder, der tilføjer en Teknisk administrator:

4.3.2 "Tilføj en Teknisk administrator" (beskrevet i afsnit 6.5).

Administrator for it-systemudbyder og Administrator for it-leverandør kan se og fjerne tekniske administratorer efter behov. Derefter skal Teknisk administrator sørge for, at de tekniske detaljer i systemet bliver klargjort til integrationstest:

4.3.3 "Indlæs tekniske data (metadata-fil)" (beskrevet i afsnit 7.7).

Under indlæsning af metadata, bliver der foretaget en automatisk validering af den uploadede XML-fil. Data skal indeholde et unikt system- eller organisations-testcertifikat, der ikke benyttes af andre NemLog-in tilslutninger, og data skal kunne valideres i forhold til OIOSAML-standarden. Teknisk administrator har også mulighed for at validere metadata fra den officielle testportal <https://test-nemlog-in.dk/testportal/> igennem metadatavalidatoren inden tilslutningen startes i NemLog-in Administrationen.

OBS: Skal systemet anvendes i forbindelse med STS - Bootstrap Token Case scenariet, se da afsnit 4.8.

Metadata skal endvidere indeholde OIOSAML privilegieattributten, som benyttes sammen med NemLog-in Brugerrettighedssystem (FBRS). For at it-systemet kan benytte <https://brugeradministration.nemlog-in.dk> i produktion, skal den tekniske administrator tilføje de privilegier, der skal indgå i løsningen:

4.3.4 "Tilføj et nyt privilegie" (beskrevet i afsnit 7.4).

Navnet på privilegiet i NemLog-in Administrationen, skal være så sigende som muligt, da det kan ses og anmodes af brugere i produktion. Privilegie-formatet skal overholde OIOSAML Basic privilegie-profilen, urn:dk:mydomain:myapp:myprivilege123 eller <https://mydomain.dk/myapp/myprivilege123>.

Integrationstestmiljøet har ikke et brugeradministrations-interface, og Teknisk administrator skal derfor tilføje testbrugere til systemet og tildele dem privilegier. Testbrugere er nødvendige uanset, om de skal modtages igennem OIOSAML assertion ved log-in, eller igennem en OIOSAML assertion ved en attribute query forespørgsel på den pågældende testbruger:

4.3.5 "Tilføj en medarbejdertestbruger" (beskrevet i afsnit 7.14 & 7.15).

Testbrugere der bliver oprettet her, vil kun være tilgængelige i integrationstestmiljøet, når systemet er overført til integrationstest. Oprettelse eller opdateres en testmedarbejder, efter systemet er flyttet i integrationstest, skal der laves en ny anmodning om integrationstest - før brugeren har de rette privilegier tilknyttet i testmiljøet.

Teknisk administrator skal nu tage stilling til it-systemets tekniske detaljer, der ikke automatisk blev opdateret ved indlæsning af metadata. Her skal der tilføjes tidspunkt for, hvornår it-systemet skal være aktivt i integrationstestmiljøet. Målgruppen for systemet, skal også defineres, da det har indflydelse på senere validering af metadata. Det udføres gennem følgende opgave:

4.3.6 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2).

Husk at trykke *Gem tekniske oplysninger*, så ændringer foretages.

Teknisk administrator kan nu ansøge om at få systemet i integrationstest. Bemærk, at det ikke er muligt at opdatere tekniske detaljer om systemet igen, før integrationstesten er godkendt eller afvist. Det unikke entityID vil desuden blive fastlåst for den specifikke tilslutning, når der er ansøgt om integrationstest, og kan ikke længere ændres. For at komme i integrationstest, skal følgende opgave udføres:

4.3.7 "Ansøg om integrationstest" (beskrevet i afsnit 7.21).

Efter anmodning om integrationstest, vil status af systemet være i *Integration test (klar)*, hvorefter system og testdata bliver overført til integrationstestmiljøet.

It-leverandør eller It-systemudbyder skal nu udføre integrationstesten i overensstemmelse med de prædefinerede testcases. Vejledning til testcases og skabelon til testrapport findes her <https://tu.nemlog-in.dk/testrapport/>. Når testen er gennemført succesfuldt, skal den tekniske administrator uploade en underskrevet testrapport:

4.3.8 "Indlæs testrapport" (beskrevet i afsnit 7.19).

Det er vigtigt at kontrollere, at testrapporten er uploadet og udfyldt korrekt før næste opgave udføres.

Når testrapporten er indlæst korrekt, skal Teknisk administrator godkende, at integrationstesten er afsluttet. Dette gøres under ventende opgaver:

4.3.9 "Håndtér en opgave" (beskrevet i afsnit 5.2).

NemLog-in supporten vil nu verificere, at testrapporten er fyldestgørende og tage stilling til, om den kan godkendes. Hvis den bliver afvist, vil systemet igen føres tilbage til status *påbegyndt*, hvorefter tidligere trin skal gentages. Hvis den bliver godkendt, vil status blive sat til *Integration test (Godkendt)*.

Systemet er nu snart klar til at blive forberedt på produktion. Dette gør Teknisk administrator ved at vælge fanen produktion og uploade nye metadata, der indeholder produktionscertifikatet:

4.3.10 "Indlæs tekniske data (metadatafil)" (beskrevet i afsnit 7.7)

Da it-systemet indeholder privilegier rettet mod NemLog-in Brugeradministration, skal NemLog-in support endvidere kontaktes på nemlogin@digst.dk i forhold til, hvordan privilegier skal indgå i rettigheder. Det er NemLog-in supporten, der opretter rettigheder og beskrivelser til rettigheder, samt mapper privilegier til en eller flere rettigheder. Rettigheder er ikke nødvendigvis systemspecifikke.

NemLog-in supporten kan oprette nødvendige rettigheder før systemet er i produktion, men kan først mappe privilegier til rettigheder, når et system er overført til produktion. Det er en god ide at kontakte NemLog-in supporten i god tid, så rettighederne er klar i før it-systemet går i drift.

Dernæst skal produktionstidspunktet for, hvornår metadata slår igennem i produktionsmiljøet angives. Dette gøres af Teknisk administrator:

4.3.11 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2)

Der er også muligt at indlæse produktionscertifikaterne her, hvis de ikke blev uploadet med ny metadata. Efter alle tekniske detaljer er opdateret, kan Teknisk administrator nu anmode om, at systemet går i produktion:

4.3.12 "Anmod om overførsel til produktion" (beskrevet i afsnit 7.22)

Status på systemet vil nu ændre sig til *Produktion (ansøgt)*. Herefter skal Administrator for it-systemudbyderen godkende, at systemet går i produktion. Det gøres under ventende opgaver:

4.3.13 "Håndtér en opgave" (beskrevet i afsnit 5.2)

Når opgaven er godkendt af It-systemudbyder, vil status på systemet være *Produktion (godkendt)*, hvorefter systemet overføres til produktion med status *Produktion (klar)*. NemLog-in supporten kan nu mappe privilegier til rettigheder, men systemet er først aktivt på det angivne tidspunkt for produktion.

Ligger produktionstidspunktet før den endelige godkendelse, kan der gå op til 5 minutter før systemet fungerer. Hvis det angivne produktionstidspunkt ligger efter den endelige godkendelse, vil systemet først fungere på det specificerede tidspunkt.

4.4 Tilslut ny Web Service Provider til STS

Dette flow beskriver hvilke opgaver der skal udføres i forbindelse med oprettelsen af en Web Service Provider (WSP) i forbindelse med anvendelse af NemLog-ins Secure Token Service (STS). Ved tilslutning af en WSP kan man vælge, om NemLog-in skal tjekke brugerens session, inden Bootstrap okens veksles mod Identity Tokens til WSP'en. Dette betyder, at en serviceaftager kun kan få et token, hvis brugeren har en aktuel session med NemLog-in IdP'en. Dette gøres ved at sætte et flueben i boksen ud for "Session check".

Bemærk at dette check kun er relevant for Bootstrap Token Case! Yderligere information omkring lokal STS og Bootstrap tokens kan findes på digitaliser.dk på følgende link: <http://digitaliser.dk/resource/526486>

For at tilslutte et nyt it-system skal Administrator for it-systemudbyder logge ind i NemLog-in Administrationen. For at oprette et nyt it-system skal administratoren først foretage følgende:

4.4.1 "Opret nyt it-system" (beskrevet i afsnit 6.4)

Det er systemtypen *Webtjeneste* der skal vælges - session check kan også tilvælges i samme tilslutning.

Det nyoprettede system vil nu få status Påbegyndt. Hvis systemet skal håndteres af en it-leverandør, skal Administratoren for it-systemudbyder tilføje denne:

4.4.1.1 "Tilføj en it-leverandør" (beskrevet i afsnit 6.8)

Herefter skal Administrator for it-leverandør udpege en eller flere tekniske administratorer. Hvis tjenesteudbyderen vil administrere deres egen tilslutning, er det i stedet Administrator for it-systemudbyder der tilføjer en Tekniskadministrator:

4.4.2 "Tilføj en Teknisk administrator" (beskrevet i afsnit 6.5)

Administrator for it-systemudbyder og Administrator for it-leverandør kan se og fjerne tekniske administratorer efter behov. Derefter skal Teknisk administrator sørge for, at de tekniske detaljer i systemet bliver klargjort til integrationstest:

4.4.3 "Indlæst tekniske data (metadata-fil)" (beskrevet i afsnit 7.7)

Formatet for metadata for en WSP adskiller sig på enkelte punkter fra det format der anvendes til systemer der anvender log-in-tjenesten (SSO). Der er på følgende sider angivet et eksempel på, hvordan WSP metadata kunne se ud:

```
<md:EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:md="dk:gov:nemlogin:ws:metadata"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xm1="http://www.w3.org/XML/1998/namespace"
entityID="https://saml.EndtoEndSTS.dk">
<md:SPWSDescriptor protocolSupportEnumeration="dk:gov:nemlogin:ws:metadata:1.0:protocol">
<md:KeyDescriptor use="encryption">
<ds:KeyInfo>
<ds:X509Data>
<!--Encryption certificate START-->
<ds:X509Certificate>MIIGKzCCBR0gAwIBAgIETBGSSDANBgqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJESzESMBAGA1UECgwJVfJVU1QyNDA4MSUw
IwYDVQQDDDBxUUUVTDIOMDggU3lzdGVzdGVzdCBWSU
IjENBMB4XDTEzMTAwTE0TE0Mjc2NloXDTE2MTAwTE0TE0Mjc2OVowZDZ0ZCZAJBgNVBAYTAkRLMSowKAYDVQQKQDCHDmGtvtbm9taXN0eXJlbHNlbiAvLyBD
VII6MTAyMTMyMzExXzAgBgNVBAUTGUNWUjoxMDIxM
zIzMS1GSUQ6NjkiMDMD5NzEwOwYDVQQDDDDTDMGtvtbm9taXN0eXJlbHNlbiBGT0NFUjYjZjX0MTAgKGZlbn0tZW9uc2NlcjRmZmRlYXQpMIIlBjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmzZWYtkGcR
/7vg8rxarqtpGT0ohQY1q2G1epgR/0d4UAMcKW4O5CYHrfA7Pt4IDWvhBs1+uDhLxS4rEeHeYHzEjHNDkLF6S/sGblHUI/RuEOVEBA25bScRH/22cwAb9K
Ui/jvYOIxxbuxl/BUo/Gm7nTBMJQfz/vtLsw+K1SXnF0oo
HbNeCDzmQotCLEuF8wPKLoYBD/QdnQxOEDVF1/Vm1wCjYeIzkgW6k1vVahN5cfpi6wFEXtj5kKxl6lizhF5KoVjgHklgDungxZ33ylAqRR+yOyGhS7BGkhQ
wo16VPcMQM3bD8XoBRlbu2SyJtREIEqKVQ8HWcjeg8dGw
IDAQABo4IcDCCAQsQwDgYDVR0PAQH/BAQDAgO4MIGUBggrBgEFBQcBAQSBhZCBhDA7BggrBgEFBQcwAYYvaHR0cDovL29jc3Auc3lzdGVtdGVzdDgu
dHJ1c3QyNDA4LmNvbS9yZXNwb25kZXIwRQYIKwYBBQUH
MAKGOWh0dHA6Ly9mLmFpYS5zeXN0ZW10ZXN0OC50cnVzdDIOMDguY29tL3N5c3RlbnRlc3Q4LWNhLmNlcjCCASAGA1UdIASCARcwggETMIIlBDwYNK
wYBBAGB9FECBAIEAJCB/TAvBggrBgEFBQcCARYjaHR0cD
ovL3d3dy50cnVzdDIOMDguY29tL3JlcG9zaXRvcnkgwGCKGCCGAQUFBwIwCMIG8MAwWBUrHbkiEMAMCAQEAgatEYW5JRCB0ZXN0IGNlcnRpZmRlYXRLci
BmcEgZGVubmUgQ0EgdWRzdGVkZXZlZG9wZDZ0ZCZAJBgNVBAYTAkRLMSowKAYDVQQKQDCHDmGtvtbm9taXN0eXJlbHNlbiAvLyBD
DEUmy42LjEuNC4xLjMxMzEzLjUuNC42LjQuMi4iGRGfU5UqgdGVzdCBjZXJ0aWZpY2F0ZXMGZnJvbSB0aGlzIENBIBGfYzSBpc3N1ZWQgdW5kZXIgdEUEU
My42LjEuNC4xLjMxMzEzLjUuNC42LjQuMi4iGwGGA1UdH
```



```

wSBozCBoDA6oDigNoY0aHR0cDovL2Nybc5zeXNOZW10ZXNOOC50cnVzdDIOMDguY29tL3N5c3RlbXRlc3Q4LmNybDBioGCgXqRcMFoxCzAJBgNVBAYT
AkRLMRIwEAYDVQQKDAIUUVTVDIOMDgxtAJBgNVBAM
MHFRSVVNUMjQwOCBtXNOZW10ZXNOIFZJSUkqQ0ExEDAOBgNVBAMMBONSTDE2MzQwHwYDVROjBBgwFoAUlhs2EzsiKcl9+ef5k+vGyz4SxwQwHQ
YDVROBBYEFpNeumvGqn5i4xuU5wSRZTQwxcYIMAKGA
1UdEwQCAAAwDQYJKoZIhvcNAQELBQADggEBAI8JepjuPBIOEHZc+GB9EvLpYoPzamNna+FOOcOZCuDJ5iLBKDJZVWL76Uhr4211oxnj+P0a9ICVdKyHtSz
ps1gF6ivHBKnypp00yqNaB9d7QCeFzwlcrnNVcWDev9e/
v4J/GkWgyPFjijwupuchKONQY4r0K77Fs4wfaBzhqrjXyL9Mr9/r98JN+gPNNfb4GwixY2IKcn81CMgJfXA4ERz7GbclcmR3p7ilgIX+1hL7/cuYDTN1kN+
QFNuo+V26EaPgsElm1ytFO2SZT0DkgnB2NSZ9veF7E/jlyns m1e34FJqO8RBOWC+nWYLyPKxMeZqqAP5Ks4aOloFmFemc=</ds:X509Certificate>

<!--Encryption certificate END-->
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://www.ads.mst.dk/myWebService.svc" ResponseLocation="http://www.mywebsite.com"
index="0" />
<md:AttributeConsumingService index="0">
<md:ServiceName xml:lang="en-US">WSP End to End STS</md:ServiceName>

<!--Common Attributes for Web service START-->
<md:RequestedAttribute FriendlyName="SpecVer" Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="AssuranceLevel" Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="surName" Name="urn:oid:2.5.4.4" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
isRequired="true" />
<md:RequestedAttribute FriendlyName="CommonName" Name="urn:oid:2.5.4.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="uid" Name="urn:oid:0.9.2342.19200300.100.1.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="serialNumber" Name="urn:oid:2.5.4.5" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="userCertificate" Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.8"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="Certificate issuer attribute" Name="urn:oid:2.5.29.29"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="CprNumberIdentifier" Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="UniqueAccountKey" Name="dk:gov:saml:attribute:UniqueAccountKey"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
</md:RequestedAttribute FriendlyName="Privileges" Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<!--Common Attributes for Web service END-->

<!--Attributes for Citizen when request is sent on behalf of a POCES Certificate START-->
<md:RequestedAttribute FriendlyName="IsYouthCert" Name="dk:gov:saml:attribute:IsYouthCert"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
<!--Attributes for Citizen when request is sent on behalf of a POCES Certificate END-->

<!--Attributes for Employees when request is sent on behalf of a MOCES Certificate START-->
<md:RequestedAttribute FriendlyName="organizationName" Name="urn:oid:2.5.4.10" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="UserAdministratorIndicator" Name="dk:gov:saml:attribute:UserAdministratorIndicator"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
<md:RequestedAttribute FriendlyName="SENumberIdentifier" Name="dk:gov:saml:attribute:SENumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />

```

```
</>
<md:RequestedAttribute FriendlyName="CvRnumberIdentifier" Name="dk:gov:saml:attribute:CvRnumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
isRequired="true" />
<md:RequestedAttribute FriendlyName="RidNumberIdentifier" Name="dk:gov:saml:attribute:RidNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
isRequired="true" />
<md:RequestedAttribute FriendlyName="OCES Pseudonym" Name="urn:oid:2.5.4.65" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic" isRequired="true" />
<!--Attributes for Employees when request is sent on behalf of a MOCES Certificate END-->
</md:AttributeConsumingService>
</md:SPWSDescriptor>
</md:EntityDescriptor>
```

Under indlæsning af metadata, bliver der foretaget en automatisk validering af den uploadede XML-fil. Data skal indeholde et unikt System- eller organisations-testcertifikat, der ikke benyttes af andre NemLog-in tilslutninger, og data skal kunne valideres i forhold til OIOSAML-standarden. Teknisk administrator har også mulighed for at validere metadata på den officielle testportal <https://test-nemlog-in.dk/testportal/> i igennem metadatavalidatoren, inden tilslutningen startes i administrationsportalen (her skal vælges "OIO WS-Trust Profile" profilen).

Teknisk administrator skal nu tage stilling til it-systemets tekniske detaljer, der ikke automatisk blev opdateret ved indlæsning af metadata. Her skal der tilføjes tidspunkt for, hvornår it-systemet skal være aktivt i integrationstestmiljøet. Målgruppen for systemet, skal også defineres, da det har indflydelse på senere validering af metadata. Det udføres gennem følgende opgave:

4.4.4 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2)

Husk at trykke *Gem tekniske oplysninger* så ændringer foretages.

Teknisk administrator kan nu ansøge om at få systemet i integrationstest. Bemærk, at det ikke er muligt at opdatere tekniske detaljer om systemet igen, før integrationstesten er godkendt eller afvist. Det unikke entityID vil desuden blive fastlåst for den specifikke tilslutning, når der er ansøgt om integrationstest, og kan ikke længere ændres. For at komme i integrationstest, skal følgende opgave udføres:

4.4.5 "Ansøg om integrationstest" (beskrevet i afsnit 7.21)

Efter anmodning om integrationstest, vil status af systemet være i *Integration test (klar)*, hvorefter system og testdata kan blive overført til integrationstestmiljøet. Data vil nu være tilgængelige i integrationstest.

It-leverandør eller It-systemudbyder skal nu udføre integrationstesten i overensstemmelse med de prædefinerede testcases. Vejledning til integrationstest for STS findes her <https://test-nemlog-in.dk/Testportal/dokumenter/NemLog-in2%20-%20STS.pdf>. Vejledning til testcases og skabelon til testrapport findes her <https://tu.nemlog-in.dk/testrapport/>

NB: Ved tilslutning af en WSP er der ikke krav om at udføre test cases. Teknisk administrator skal derfor uploade en tom testrapport:

4.4.6 "Indlæs testrapport" (beskrevet i afsnit 7.19)

Det er vigtigt at kontrollere, at testrapporten er uploadet og udfyldt korrekt før næste opgave udføres.

Når testrapporten er indlæst korrekt, skal Tekniske administrator godkende, at integrationstesten er afsluttet. Dette gøres under ventende opgaver:

4.4.7 "Håndtér en opgave" (beskrevet i afsnit 5.2)

NemLog-in supporten vil nu verificere, at testrapporten er fyldestgørende og tage stilling til, om den kan godkendes. Hvis den bliver afvist, vil systemet igen føres tilbage til status *påbegyndt*, hvorefter tidligere trin skal gentages. Hvis den bliver godkendt, vil status blive sat til *Integration test (gennemført)*.

Systemet er nu snart klar til at blive forberedt på produktion. Dette gør Teknisk administrator ved at vælge fanen produktion og uploade nye metadata, der indeholder produktionscertifikatet:

4.4.8 "Indlæs tekniske data (metadatafil)" (beskrevet i afsnit 7.7)

Dernæst skal produktionstidspunktet for, hvornår metadata slår igennem i produktionsmiljøet angives. Dette gøres af Teknisk administrator:

4.4.9 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2)

Der er også muligt at indlæse produktionscertifikaterne her, hvis de ikke blev uploadet med ny metadata. Efter alle tekniske detaljer er opdateret, kan Teknisk administrator nu anmode om, at systemet går i produktion:

4.4.10 "Anmod om overførsel til produktion" (beskrevet i afsnit 7.22)

Status på systemet vil nu ændre sig til *Produktion (ansøgt)*. Herefter skal Administrator for it-systemudbyderen godkende, at it-systemet går i produktion. Det gøres under ventende opgaver:

4.4.11 "Håndtér en opgave" (beskrevet i afsnit 5.2)

Når opgaven er godkendt af It-systemudbyder, vil status på systemet være *Produktion (godkendt)*, hvorefter systemet overføres til produktion med status *Produktion (klar)*. NemLog-in supporten kan nu tilføje privilegier til rettigheder, men systemet er først aktivt på det angivne tidspunkt for produktion.

Ligger produktionstidspunktet før den endelige godkendelse, kan der gå op til 5 minutter før systemet fungerer. Hvis det angivne produktionstidspunkt ligger efter den endelige godkendelse, vil systemet først fungere på det angivne tidspunkt.

4.5 Tilslut nyt it-system til log-in-tjenesten (SSO) der indeholder fuldmagtsprivilegier rettet mod borgere

En tilslutning til log-in-tjenesten (SSO), der skal benyttes igennem NemLog-in Borgerfuldmagtsløsning, skal indeholde OIOSAML privilegie attributten, og fuldmagtsprivilegier skal være oprettet i NemLog-in Administration. Fuldmagtspakker kan endvidere oprettes i NemLog-in Brugeradministration, som beskrevet i dette flow.

For at tilslutte et ny it-system skal Administrator for it-systemudbyder logge ind i administrationsportalen. For at oprette et nyt it-system skal administratoren først oprette systemet:

4.5.1 "Opret nyt it-system" (beskrevet i afsnit 6.4)

Der er systemtype log-in service (SSO), der skal vælges - Signeringstjeneste kan også vælges i samme tilslutning. Det nyoprettede system vil nu få status *Påbegyndt*. Hvis det nyoprettede system, skal håndteres af en it-leverandør, skal Administratoren for it-systemudbyder tilføje en it-leverandør:

4.5.1.1 "Tilføj en it-leverandør" (beskrevet i afsnit 6.8)

Administrator for it-leverandør skal nu udpege en eller flere tekniske administratorer. Hvis tjenesteudbyderen vil administrere deres egen tilslutning, er det i stedet Administrator for it-systemudbyder, der skal tilføje en Teknisk administrator:

4.5.2 "Tilføj en teknisk administrator" (beskrevet i afsnit 6.5)

Administrator for it-systemudbyder og Administrator for it-leverandør kan se og fjerne tekniske administratorer efter behov. Herefter skal Teknisk administrator sørge for, at de tekniske detaljer om systemet bliver klargjort til integrationstest:

4.5.3 "Indlæs tekniske data (metadatafil)" (beskrevet i afsnit 7.7)

Under indlæsning af metadata bliver den uploadede XML fil automatisk valideret. Data skal indeholde et unikt System- eller organisations-testcertifikat, der ikke bliver benyttet af andre NemLog-in tilslutninger, og data skal kunne valideres i forhold til OIOSAML-standard

Teknisk administrator har også mulighed for at validere metadata fra den officielle testportal <https://test-nemlog-in.dk/testportal/> igennem metadatavalidatoren, inden tilslutningen startes i NemLog-in Administrationen. Metadata skal endvidere indeholde OIOSAML privilegieattributten, da den skal benyttes sammen med den fællesoffentlige fuldmagtsløsning, Digital Fuldmagt. For at it-systemet i produktion kan benytte <https://fuldmagt.nemlog-in.dk>, skal Teknisk administrator tilføje de fuldmagtsprivilegier, der skal indgå i løsningen:

4.5.4 "Tilføj et nyt privilegie" (beskrevet i afsnit 7.3)

Navnet på fuldmagtsprivilegiet i NemLog-in Administrationen, skal være så sigende som muligt, da det kan ses og anmodes af brugere i produktion. Privilegie-formatet skal overholde OIOSAML Basic privilegieprofilen, <urn:dk:mydomain:myapp:myprivilege123> eller <https://mydomain.dk/myapp/myprivilege123>

Integrationstestmiljøet indeholder ikke brugeradministration eller fuldmagtinterface, derfor skal Teknisk administrator tilføje testbrugere til systemet og knytte dem til privilegier. Testbrugere er nødvendige, uanset om de skal modtages igennem OIOSAML assertion ved log-in eller igennem en OIOSAML assertion ved en attribute query forespørgsel på den pågældende testbruger. Der skal både tilføjes medarbejder- og borgertestbrugere:

4.5.5 "Tilføj en borgertestbruger" (beskrevet i afsnit 7.12 & 7.13)

4.5.6 "Tilføj en medarbejdertestbruger" (beskrevet i afsnit 7.14 & 7.15)

Testbrugere der bliver oprettet her, vil kun være tilgængelige i integrationstestmiljøet, efter systemet bliver overført til integrationstest. Oprettelse eller opdateres en testbruger efter, at systemet er flyttet i integrationstest, skal der foretages en ny anmodning om integrationstest før brugeren har de rette fuldmagtsprivilegier tilknyttet i testmiljøet.

Teknisk administrator skal nu tage stilling til it-systemets tekniske detaljer, der ikke automatisk blev opdateret ved indlæsning af metadata. Fx skal der tilføjes tidspunkt for, hvornår tilslutning for it-system skal være aktivt i integrationstestmiljøet. Det skal også defineres om systemet skal understøtte NemID/MitID Privat til Erhverv. Endvidere skal det defineres, hvordan fuldmagtsprivilegier ønskes udstedt. Det gøres ved at opdatere de tekniske data:

4.5.7 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2)

Husk at trykke *Gem tekniske oplysninger*, så ændringer foretages.

Ønsker du at benytte fuldmagtsservicen, samt at denne service benytter et andet System- eller organisations-certifikat end log-in-tjenesten (SSO), kan det defineres, efter du har valgt, at fuldmagtprivilegier kan udstedes igennem fuldmagtsservicen. Teknisk administrator skal i dette tilfælde administrere adgang til fuldmagtstjenesten:

4.5.8 "Administrer adgang til fuldmagtstjenesten" (beskrevet i afsnit 7.3)

Bemærk, at du her både skal angive et unikt System- eller organisations-testcertifikat og et unikt produktionscertifikat.

Teknisk administrator kan nu ansøge om at få systemet i integrationstest. Det er ikke muligt at opdatere tekniske detaljer om systemet, før integrationstesten er enten godkendt eller afvist. Det unikke entityID bliver desuden fastlåst for den specifikke tilslutning, når der er ansøgt om integrationstest. For at komme i integrationstest, skal der ansøges herom:

4.5.9 "Ansøg om integrationstest" (beskrevet i afsnit 7.21)

Efter anmodning om integrationstest, vil status af systemet være i Integration test

(klar), hvorefter system og testdata bliver overført til integrationstestmiljøet. Data vil nu være tilgængelige i integrationstest og status på systemet vil nu være Integration test (klar).

It-leverandør eller It-systemudbyder skal nu udføre integrationstesten i overensstemmelse med de prædefinerede testcases. Vejledning til testcases og skabelon til testrapport findes her <https://tu.nemlog-in.dk/testrapport/>.

Når testen er gennemført succesfuldt, skal Tekniske administrator uploade en underskrevet testrapport:

4.5.10 "Indlæs testrapport" (beskrevet i afsnit 7.19)

Det er vigtigt at kontrollere, at testrapporten er uploadet og udfyldt korrekt.

Når Testrapport er indlæst korrekt, skal Teknisk administrator godkende, at integrationstesten er afsluttet. Dette gøres ved at godkende den opgave, der ligger under ventende opgaver:

4.5.11 "Håndtér en opgave" (beskrevet i afsnit 5.2)

NemLog-in supporten skal nu verificere, at testrapporten er fyldestgørende og tage stilling til, om den kan godkendes. Hvis den bliver afvist, vil systemet føres tilbage til status *påbegyndt*, hvorefter tidligere trin gentages. Hvis den bliver godkendt, bliver status sat til *Integration test* (Godkendt).

Systemet er nu snart klar til at blive forberedt til produktion. Det gør Teknisk administrator ved at uploade nye metadata, der indeholder produktionscertifikatet:

4.5.12 "Indlæs tekniske data (metadatafil)" (beskrevet i afsnit 7.7)

Da it-systemet indeholder fuldmagtsprivilegier rettet mod NemLog-in Brugeradministration, skal NemLog-in support endvidere kontaktes på nemlogin@digst.dk, hvis fuldmagtsprivilegier skal indgå i fuldmagtspakker. Det er NemLog-in supporten der opretter fuldmagtspakker, der kan benyttes i borgerfuldmagtsløsningen, samt mapper fuldmagtsprivilegier til fuldmagtspakker. Fuldmagtspakker er ikke systemspecifikke.

NemLog-in supporten kan oprette nødvendige fuldmagtspakker efter behov, men kan først mappe fuldmagtsprivilegier til fuldmagtspakker, når et system er overført til produktion. Det er en god ide at kontakte NemLog-in supporten i god tid, hvis fuldmagtsprivilegier skal indgå i fuldmagtspakker. Læs mere om fuldmagtsløsningen her: <https://www.digitaliser.dk/resource/5880352>

Dernæst skal produktionstidspunktet angives for, hvornår metadata skal slå igennem i produktionsmiljøet. Det gør Teknisk administrator:

4.5.13 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2)

Det er her muligt at indlæse produktionscertifikaterne, hvis de ikke blev uploadet med ny metadata. Efter alle tekniske detaljer er opdateret, kan Teknisk administrator nu anmode om at systemet går i produktion.

4.5.14 "Anmod om overførsel til produktion" (beskrevet i afsnit 7.22)

Status på systemet vil nu ændre sig til *Produktion (ansøgt)*.

Herefter skal Administrator for it-systemudbyderen godkende, at it-systemet går i produktion. Det gøres fra ventende opgaver:

4.5.15 "Håndtér en opgave" (beskrevet i afsnit 5.2)

Når opgaven er godkendt af tjenesteudbyderen, vil status på systemet være Produktion (godkendt).

Da it-systemet indeholder fuldmagtsprivilegier, der er synlige for alle borgere, skal NemLog-in supporten også godkende, at systemet kan overføres til produktion.

Herefter bliver systemet overført til produktion med status *Produktion (klar)*. NemLog-in supporten vil nu have mulighed for at tilføje fuldmagtsprivilegier til fuldmagtspakker, men systemet vil først være aktivt på det angivne tidspunkt for produktion.

I tilfælde af, at produktionstidspunkt ligger før den endelige godkendelse, kan der gå op til 5 minutter før systemet vil fungere. Hvis det angivne produktionstidspunkt ligger efter den endelige godkendelse, vil systemet fungere på det angivne tidspunkt.

4.6 Opdater eksisterende tilslutning til log-in-tjenesten (herunder certifikatudskiftning)

Efter it-systemet er kommet i produktion med status *Produktion (klar)*, vil der ofte opstå behov for at opdatere systemdetaljer i forhold til den tilsluttede version.

Den typiske årsag vil ofte være, at system- eller organisations-certifikatet skal udskiftes, eller der skal oprettes en ny version til testformål - mens den tidligere version forbliver i produktion.

En anden årsag kunne være at it-systemet skal kunne anvendes i forbindelse med STS. For at kunne anvende Bootstrap Token scenariet skal metadata opdateres med attributten <https://data.gov.dk/model/core/eid/bootstrapToken> for at der kan udstedes en Bootstrap token. Yderligere information omkring Bootstrap tokens kan findes på følgende link:

<https://digst.dk/media/23391/oiosaml-web-sso-profile-302.pdf>

Det er Teknisk administrator, der skal opdatere systemdetaljer ved at ved at oprette en ny version af teknisk data:

4.6.1 "Opret en ny version af teknisk data (metadata)" (beskrevet i afsnit 7.11)

Den tidligere version, der er i produktion, forbliver i produktion, indtil der anmodes om at få den nye version i produktion igennem godkendelsesprocessen for en ny tilslutning. Så snart en ny version er oprettet, vises den med et nyt versionsnummer og med *status: Påbegyndt*.

Bemærk, at migrerede systemer kan indeholde metadata, der ikke lever op til de nuværende valideringsregler. I dette tilfælde skal metadata opdateres, så de lever op til OIOSAML standarderne, før den nye version kan sættes i produktion.

Hvis man blot skal skifte produktionscertifikatet, kan Teknisk administrator gøre dette ved at indlæse nye metadata der indeholder det nye unikke system- eller organisations- produktionscertifikat eller ved at trykke på 'Skift Certifikat' linket (beskrevet i afsnit 7.21).

4.6.2 Indlæs tekniske data (metadata) (beskrevet i afsnit 7.7)

Hvis der ved oprettelsen af den nye version er valgt at bibeholde eksisterende metadata, kan man vedligeholde metadata ved at opdatere de tekniske data, som indgår i næste trin.

Dernæst skal Produktionstidspunktet angives for, hvornår metadata slår igennem i produktionsmiljøet. Det er Teknisk administrator, der skal opdatere teknisk data:

4.6.3 "Rediger tekniske oplysninger om it-systemet" (beskrevet i afsnit 7.2)

Det er her muligt at indlæse produktioncertifikaterne, hvis de ikke blev uploadet med ny metadata. Det gøres ved at vælge menupunktet "Skift certifikat" i Løs opgaver menuen (beskrevet i afsnit 7.21). Det ønskede certifikat skal herefter indlæses fra en .CER fil.

Så snart systemet er i version 2 eller højere, er der ikke et systemteknisk krav om at en ny version skal i integrationstest, før der kan anmodes om produktion. Teknisk administrator kan derfor anmode om, at systemet går i produktion:

4.6.4 "Anmod om overførsel til produktion" (beskrevet i afsnit 7.20)

Status på systemet vil nu ændre sig til Produktion (ansøgt).

Herefter skal Administrator for it-systemudbyderen under *Ventende opgaver* godkende, at it-systemet går i produktion:

4.6.5 "Håndtér en opgave" (beskrevet i afsnit 5.2)

Når opgaven er godkendt af it-systemudbyder, vil status på systemet være *Produktion* (godkendt). Løsningen vil herefter automatisk komme i status *Produktion (klar)*.

Ligger produktionstidspunkt før den endelige godkendelse, kan der gå op til 5 minutter, før systemet vil fungere efter den endelige godkendelse af it-systemudbyder. Hvis det angivne produktionstidspunkt ligger efter den endelige godkendelse, vil systemet fungere på angivne tidspunkt.

Bemærk, at systemet også skal godkendes af NemLog-in support, hvis det indeholder fuldmagts privilegier.

Hvis den nye version af systemet skal benyttes til mere end udskiftning af certifikat, skal der udføres integrationstest. Det vil her være nødvendigt at udskifte certifikatet med et MOCES eller VOCES-testcertifikat. Certifikater der tidligere er benyttet for dette entityID kan benyttes, men certifikatet skal være unikt i NemLog-in. Udskiftning foretages på samme måde som beskrevet i trin 1.

For at flytte den nye udgave af it-systemet til integrationstest, skal Teknisk administrator ansøge herom:

4.6.6 "Ansøg om integrationstest" (beskrevet i afsnit 7.21)

De opdaterede metadata og eventuelt testdata bliver flyttet til integrationstestmiljøet, når administrator modtager besked herom. Bemærk, at status stadig vil være *Påbegyndt*, når den nye version er flyttet til integrationstest.

Oprettes der nye testdata eller laves en ændring til metadata, skal den tekniske administrator gentage ansøgning om integrationstest. Der er ikke nogen begrænsning for ansøgning om integrationstest for en ny version af et system - så længe systemet er i status *Påbegyndt*.

Selv om der er oprettet en ny version af systemet, vil tidligere tekniske detaljer om produktionsversioner stadig være tilgængelige for den tekniske administrator:

4.6.7 "Se versioner af teknisk data (metadata)" (beskrevet i afsnit 7.10)

4.7 Oprettelse af Lokal STS – Local Token Case

For brugerscenariet Local Token Case hvor en brugerorganisation (WSC) har brug for at oprette en lokal STS i forbindelse med anvendelse af STS skal NemLog-in support kontaktes på nemlogin@digst.dk. Oprettelse af en Lokal STS skal foretages i Nemlog-in/ Administration, men kan kun foretages af NemLog-in administrator rollen. Ved oprettelse af en Lokal STS skal der anvendes et Entity ID og et test signeringscertifikat og et produktions signeringscertifikat. Disse certifikater skal være af typen system eller organisation.

4.8 Opdatering af metadata for anvendelse af STS – Bootstrap Token Case

I scenariet Bootstrap Token Case bliver brugerens identitet godkendt på baggrund af et Bootstrap Token som udstedes af Nemlog-In WebSSO som et resultat af et gennemført login transaktion. Dette Bootstrap Token anvendes så til at kontakte en STS for at få udstedt et token til en webservice. Yderligere information omkring Bootstrap tokens kan findes på *digitaliser.dk* på følgende link: <http://digitaliser.dk/resource/526486>

For at kunne indlejre denne attribut i en SAML assertion og dermed udstede et Bootstrap Token kræves det at metadata indeholder attributten: *urn:liberty:disco:2006-08:DiscoveryEPR*. Som Web Service Consumer (WSC) er det derfor nødvendigt at opdatere metadata i CSS.

Eksisterende it-systemer som ikke tidligere har anvendt en STS vil derfor skulle opdatere metadata med denne specifikke attribut.

4.9 Registrering i CSS – Signature Case

I dette scenario bliver bruger identiteten garanteret af brugeren som signerer anmodningen til Nemlog-In STS med brugerens MOCES certifikat. Brugeren skal tilhøre en brugerorganisation der er registreret i CSS.

Web Service Consumer består i dette scenario af en given applikation og der oprettes ingen tillid mellem WSC og Nemlog-In STS.

4.10 Oprette og vedligeholde tekniske data for en systembruger

Denne sektion beskriver hvordan en teknisk administrator for en brugerorganisation eller en service udbyder kan registrere og vedligeholde en systembruger.

For at oprette eller vedligeholde en ny systembruger skal den tekniske administrator for en brugerorganisation eller en service udbyder logge ind i administrationsportalen.

4.10.1 "Opret ny systembruger" (beskrevet i afsnit 7.24)

4.10.2 "Vedligehold systembruger" (beskrevet i afsnit 7.25)

Den tekniske administrator kan redigere de tekniske oplysninger for en systembruger.

4.10.3 "Provisioner systembruger til integrationstest" (beskrevet i afsnit 7.26)

Når systembrugeren er provisioneret til integrationstest miljøet kan testen påbegynde.

4.10.4 "Provisioner systembruger til produktion" (beskrevet i afsnit 7.27)

Når systembrugeren er provisioneret til produktion er det muligt at benytte denne i produktionsmiljøet

4.10.5 "Skift systembruger ejer" (beskrevet i afsnit 7.28)

Man kan skifte brugerorganisation for en systembruger, denne menu vil dog kun være tilgængelig for en KFOBS Administrator.

4.10.6 "Anmod om webservice adgang" (beskrevet i afsnit 7.29)

En systembruger kan anmode om at få adgang til en webservice hvis servicen supportere systembrugere samt den kun tillader godkendte systembrugere. Hvis servicen tillader alle systembrugere er det naturligvis ikke nødvendigt at søge om adgang.

4.10.7 "Supporter systembruger" (beskrevet i afsnit 7.30)

Under oprettelse af webservicen kan det bestemmes om servicen skal supportere brug af systembrugere. Ligeledes kan man vælge om det skal være alle systembrugere som får adgang eller om det kun er godkendte systembrugere.

4.10.8 "Godkend eller afvis systembrugeranmodning til webservice" (beskrevet i afsnit 7.31)

Når en systembruger sender en anmodning til at få adgang til en webservice bliver der genereret en opgave til service udbyderens administrator. Administratoren kan nu godkende eller afvise anmodningen.

4.10.9 Tildel og fjern system privilegier til systembrugere" (beskrevet i afsnit 7.32)

Man kan tildele og fjerne system privilegier til systembrugere. Dette gøres fra menuen under web servicen. Her er det også muligt at fjerne en systembrugers adgang til web servicen.

4.10.10 "Tilføj test systembrugere" (beskrevet i afsnit 7.33)

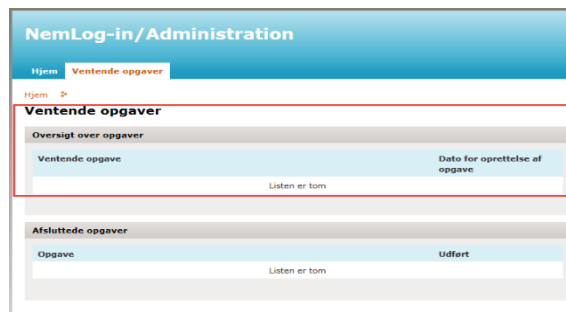
Man kan tilføje test systembrugere til en webservice og tildele brugerne privilegier.

5 Ventende opgaver

5.1 Se ventende opgaver

1

Åbn opgaver. Klik på 'Ventende opgaver' i hovedmenuen for at se en liste af de opgaver, som er tildelt dig.



2

Se opgaver. På siden ses en oversigt over fuldførte opgaver under 'Afsluttede opgaver'. De opgaver du mangler, står under 'Oversigt over opgaver'. Når du har afsluttet en opgave flyttes den automatisk til 'Afsluttede opgaver'.



Funktionen er tilgængelig for rollerne:

- Administrator for it-systemudbyder.
- Teknisk administrator

5.2 Håndtér en opgave

1

Åbn opgaver. Klik på 'Ventende opgaver' i hovedmenuen for at se en liste af de opgaver, som er tildelt dig.



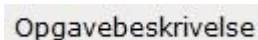
2

Åbn opgave. Klik på en opgave under 'Oversigt over opgaver'.

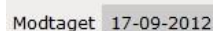
Manuel godkendelse af brugerorganisation, hvor underskriftsbemyndiget ikke kunne verificeres via CVR, for JENS YTZEN, SÆDDING A/S

3

Læs opgavebeskrivelse. Læs opgavebeskrivelsen grundigt, inden du fuldfører opgaven. Det er muligt, at du for at fuldføre opgaven, er nødt til at udføre handlinger andre steder i Administrationen eller i andre it-værktøjer.



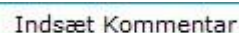
Du kan se en beskrivelse af opgaven under 'Opgavebeskrivelse', samt hvornår opgaven er modtaget.



Hvis personer tidligere i arbejdsgangen har tilføjet noter til deres opgaver, vil disse fremgå under 'Tidligere kommentarer'.

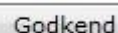


Hvis du har en kommentar til din udførsel af opgaven eller en begrundelse for, hvorfor du afviser at udføre den, kan du skrive dette ved at klikke på 'Indsæt Kommentar' og skrive i tekstfeltet.



4

Godkend opgave. De fleste opgaver giver dig mulighed for enten at godkende eller afvise, at opgaven er fuldført. Hvis du har godkendt, at opgaven fuldføres, fortsætter tilslutningsprocessen. Hvis du derimod vælger at afvise opgaven, vil arbejdsgangen starte forfra.



5

Bekræft fuldførelse. Klik på 'OK' for at fuldføre opgaven.



Funktionen er tilgængelig for rollerne:

- Administrator for it-systemudbyder.
- Teknisk administrator

5.3 Opgaver til administrator for it-systemudbyder

Følgende opgaver kan opstå til Administrator for it-systemudbyder i forhold til administration af et it-system:

Når en Teknisk administrator af et it-system anmoder om, at en ny version skal overføres til integrationstest, får Administrator for it-systemudbyder en opgave. Opgaven oprettes, når der anmodes om at få systemet overført til integrationstest, hvis systemet er i version 1. Godkendelse af opgaven er en forudsætning for, at systemet kan overføres til integrationstestmiljøet og kan kun gennemføres af Administrator for it-systemudbyder .

Når en Teknisk administrator anmoder om, at en ny version af et system skal overføres til produktion, får Administratoren for it-systemudbyder en opgave. Godkendelse af opgaven er en forudsætning for, at systemet kan overføres til produktion og kan kun gennemføres af Administrator for it-systemudbyder .

6 Håndtering af it-systemer

6.1 Se oversigt over it-systemer

1

Gå til Hjem. Klik på 'Hjem' i hovedmenuen.

Se oversigt. Klik på 'Hjem' i hovedmenuen.



2

Se oversigt. Oversigten over it-systemer vises.

Oversigten indeholder følgende informationer:

- it-systemet (navn)
- it-systemudbyder
- Status for tilslutning af it-systemet
- Nemlog-in komponenter i brug
- Dato for udløb af certifikat

Det er muligt at sortere oversigten ved at klikke på kolonnenavnet:

It-systemet ▲	It-systemudbyder	Status for tilslutning	Nemlog-in komponenter	Certifikat udløb
---------------	------------------	------------------------	-----------------------	------------------

Det er muligt at søge i oversigten via søgefunktionaliteten. Det er endvidere muligt at bladre frem og tilbage i oversigten via sidevælgerne i bunden af systemoversigten:

Resultater pr. side: 20 ▼	1 2 3 4 > >>	Viser 1 - 20 af 64
---------------------------	--------------	--------------------

Status for tilslutning af it-systemet vises både med en tekststatus, fx 'Påbegyndt', og som en visuel præsentation, som gør det nemt at danne sig et overblik over, hvor it-systemerne i oversigten er i deres tilslutningsproces:

Hjem ✖ It-systemer It-systemer It-systemudbyder		It-systemer Søg i oversigten: Søg <table> <tr> <th>It-systemet ▲</th><th>It-systemudbyder</th><th>Status for tilslutning</th><th>Nemlog-in komponenter</th><th>Certifikat udløb</th></tr> <tr> <td>IT- og Telestyrelsen System 10</td><td>IT- og Telestyrelsen</td><td>Produktion (klar)</td><td>Web sso Normalt Privilege</td><td>23-01-2018</td></tr> <tr> <td>IT- og Telestyrelsen System 11</td><td>IT- og Telestyrelsen</td><td>Påbegyndt</td><td>Web sso Fuldmagt Privilege Normalt Privilege</td><td></td></tr> <tr> <td>IT- og Telestyrelsen System 17</td><td>IT- og Telestyrelsen</td><td>Produktion (klar)</td><td>Web sso Fuldmagt Privilege</td><td>22-01-2018</td></tr> <tr> <td>IT- og Telestyrelsen System 21</td><td>IT- og Telestyrelsen</td><td>Produktion (klar)</td><td>Web sso Fuldmagt Privilege Normalt Privilege</td><td>23-01-2018</td></tr> </table>			It-systemet ▲	It-systemudbyder	Status for tilslutning	Nemlog-in komponenter	Certifikat udløb	IT- og Telestyrelsen System 10	IT- og Telestyrelsen	Produktion (klar)	Web sso Normalt Privilege	23-01-2018	IT- og Telestyrelsen System 11	IT- og Telestyrelsen	Påbegyndt	Web sso Fuldmagt Privilege Normalt Privilege		IT- og Telestyrelsen System 17	IT- og Telestyrelsen	Produktion (klar)	Web sso Fuldmagt Privilege	22-01-2018	IT- og Telestyrelsen System 21	IT- og Telestyrelsen	Produktion (klar)	Web sso Fuldmagt Privilege Normalt Privilege	23-01-2018
It-systemet ▲	It-systemudbyder	Status for tilslutning	Nemlog-in komponenter	Certifikat udløb																									
IT- og Telestyrelsen System 10	IT- og Telestyrelsen	Produktion (klar)	Web sso Normalt Privilege	23-01-2018																									
IT- og Telestyrelsen System 11	IT- og Telestyrelsen	Påbegyndt	Web sso Fuldmagt Privilege Normalt Privilege																										
IT- og Telestyrelsen System 17	IT- og Telestyrelsen	Produktion (klar)	Web sso Fuldmagt Privilege	22-01-2018																									
IT- og Telestyrelsen System 21	IT- og Telestyrelsen	Produktion (klar)	Web sso Fuldmagt Privilege Normalt Privilege	23-01-2018																									

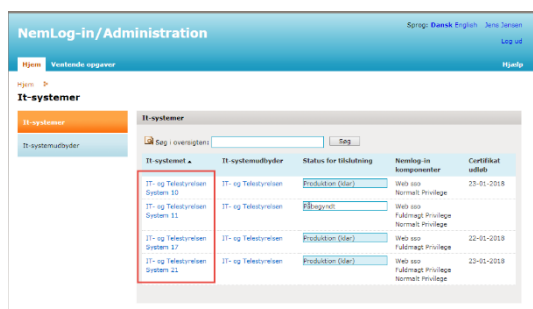
Funktionen er tilgængelig for rollerne:

- Teknisk administrator

6.2 Se detaljer for it-system

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



Søgefunktionen kan også med fordel bruges. Hvis det ønskede it-system ikke findes, kan det skyldes, at det endnu ikke er oprettet eller at du ikke er tilføjet som tekniskadministrator.

2

Se stamdata. De generelle oplysninger om it systemet kan ses ved at klikke på 'Stamdata', hvorved disse data foldes ud.

Følgende oplysninger vises:

- it-systemnavn
- Kort beskrivelse af it-systemet (hvad kan slutbrugerne benytte det til)
- Kort engelsk beskrivelse af it-systemet
- it-systemtype
- it-systemudbyder
- Tilslutningsstatus for seneste version af metadata registreret i NemLog-in
- Status for seneste version af metadata registreret hos NemLog-in.



Hjem » It-systemer » IT- og Telestyrelsen System 11

It-systemer

It-systemudbyder

Løs opgaver

[Tilføj ny it-leverandør](#)

[Tilføj teknisk administrator](#)

[Rediger tekniske oplysninger om it-systemet](#)

[Slet it-systemet](#)

Stamdata for it-system

It-systemnavn: IT- og Telestyrelsen System 11

It-systemtype: Web sso

It-systemudbyder: IT- og Telestyrelsen

Tilslutningsstatus for seneste version af metadata registreret hos NemLog-in: Påbegyndt

Status for seneste version af metadata registreret hos NemLog-in: 3

Gem stamdata

Om IT- og Telestyrelsen System 11

Teknisk adm... | It-leverandør | Metadater... | Systembrug...

IT- og Telestyr... har følgende tekniske administratorer

Fulde navn	E-mail	Telefonnummer	Organisationsnavn
Jens Jensen	JensJensen1@kfobs.dk		IT- og Telestyrelsen Fjern
Jeppe Jeppesen	JeppeJeppesen@kfobs.dk		IT- og Telestyrelsen Fjern

3

Se tilknytninger til it-system. I området 'Om it-system', fx Om

Bibliotekssystem, er det muligt at

se flere oplysninger om it-systemet. Det er muligt at se:

- **Teknisk administrator** (hvilke tekniske administratorer har it-systemet og i hvilken organisation de sidder)
- **it-leverandør** (Hvilke it-leverandører har it-systemet tilknyttet)
- **Metadatatversioner** (Hvilken livscyklus har it-systemet været igennem). Det er herfra også muligt at hente metadata fra tidligere versioner.

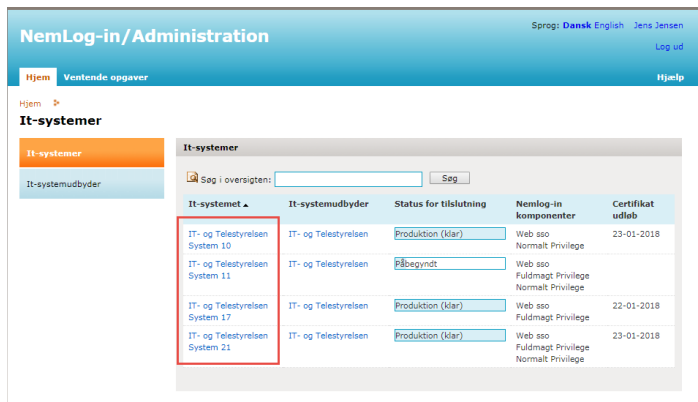
Funktionen er tilgængelig for rollerne:

- Administrator for it-systemudbyder
- Administrator for it-leverandør
- Teknisk administrator

6.3 Opdater oplysninger om it-system

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



Søgefunktionen kan også med fordel bruges. Hvis det ønskede it-system ikke findes, kan det skyldes, at det endnu ikke er oprettet eller at du ikke er tilføjet som teknisk administrator.

2

Åbn stamdata. Klik på 'Stamdata' på en side for detaljer om et it-system.



3

Opdatér oplysninger. Indsæt de korrekte stamdata for it-systemet i felterne. Det er muligt at ændre i følgende data:

- it-systemnavn
- Kort beskrivelse af it-systemet (hvad kan slutbrugerne benytte det til)
- Kort engelsk beskrivelse af it-systemet.

Stamdata for it-system

It-systemnavn
IT- og Telestyrelsen System 11

Kort beskrivelse af it-systemet (hvad kan slutbrugerne benytte det til)
IT- og Telestyrelsen System 11

Kort engelsk beskrivelse af it-systemet
IT- og Telestyrelsen System 11

It-systemtype
Web sso

It-systemudbyder
IT- og Telestyrelsen

Tilslutningsstatus for seneste version af metadata registreret hos NemLog-in
Påbegyndt

Status for seneste version af metadata registreret hos NemLog-in
3

Gem stamdata

4

Gem ændringer. Klik på 'Gem stamdata' for at opdatere oplysningerne om it-systemet.

Funktionen er tilgængelig for rollerne:

- Administrator for it-systemudbyder
- Administrator for it-leverandør
- Teknisk administrator

6.4 Opret nyt it-system

1

Gå til Hjem. Klik på 'Hjem' i hovedmenuen.



2

Opret. Klik på 'Opret nyt it-system' i menuen 'Løsopgaver' til venstre.

3

Indtast oplysninger om it-systemet. It-systemnavn. Du bør også tilføje en kort

beskrivelse af it-systemet af hensyn til
andrebrugeres forståelse.

4

A. Offentlig it-systemudbyder eller Broker

Opret. Angiv NemLog-in komponenter. Vælg hvilke NemLog-in komponenter, som it-systemet skal anvende. Du kan vælge imellem:

- Log-in-tjeneste (SSO) – OIOSAML 2
- Signeringstjeneste (legacy)
- Web Service Provider – OIO SAML 3
- Kvalificeret signeringstjeneste
- Offentlig Broker (sikringsniveau – betydelig)
- Offentlig Broker (sikringsniveau – høj)
- Web Service Provider – OIOSAML 3

Angiv hvilke NemLog-in komponenter it-systemet skal anvende

Angiv hvilke NemLog-in komponenter it-systemet skal anvende *

☐ Log-in-tjeneste (SSO) - OIOSAML 2 ⓘ

☐ Signeringstjeneste (legacy)

☐ Signeringstjeneste (legacy) ⓘ

☐ Web Service Provider - OIOSAML 2 ⓘ

☐ Sessionstjek (WS-Trust)

☐ Web SSO, OIO SAML 3 ⓘ

☐ Signeringstjeneste (legacy)

☐ Kvalificeret signeringstjeneste

☐ Kvalificeret signeringstjeneste ⓘ

☐ Offentlig broker (sikringsniveau – betydelig) ⓘ

☐ Kvalificeret signeringstjeneste

☐ Avancerede brokertjenester

☐ Services til brokers egen signeringsklient

☐ Offentlig broker (sikringsniveau – høj) ⓘ

☐ Kvalificeret signeringstjeneste

☐ Avancerede brokertjenester

☐ Services til brokers egen signeringsklient

☐ Web Service Provider - OIOSAML 3 ⓘ

☐ Sessionstjek (WS-Trust)

Få mere information om de forskellige typer ved at
holde markøren over de gule spørgsmålstegn.



B. Privat it-systemudbyder eller Broker

Opret. Angiv NemLog-in komponenter. Vælg hvilke NemLog-in komponenter, som it-systemet skal anvende. Du kan vælge imellem:

- Log-in-tjeneste (privat) – OIOSAML 3
- Kvalificeret signeringstjeneste
- Privat Broker (sikringsniveau – betydelig)
- Privat Broker (sikringsniveau – høj)

Angiv hvilke NemLog-in komponenter it-systemet skal anvende

Angiv hvilke NemLog-in komponenter it-systemet skal anvende *

☐ Log-in-tjeneste (privat) - OIOSAML 3 ⓘ

☐ Kvalificeret signeringstjeneste

☐ Kvalificeret signeringstjeneste ⓘ

☐ Privat broker (sikringsniveau – betydelig) ⓘ

☐ Kvalificeret signeringstjeneste

☐ Avancerede brokertjenester

☐ Services til brokers egen signeringsklient

☐ Privat broker (sikringsniveau – høj) ⓘ

☐ Kvalificeret signeringstjeneste

☐ Avancerede brokertjenester

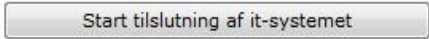
☐ Services til brokers egen signeringsklient

Få mere information om de forskellige typer ved at
holde markøren over de gule spørgsmålstegn.



5

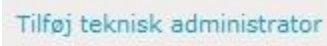
Start tilslutning. Klik på 'Start tilslutning af it systemet', når formularen er udfyldt.

Start tilslutning af it-systemet**Bemærk!**

Hvis den valgte it-systemudbyder ikke har de gældende vilkår for brug af NemLog-in, er det ikke muligt at sætte systemet i produktion. Det vil dog være muligt at oprette systemet, så tekniske data kan indsættes. Tilslutning vil gøre dig opmærksom på dette og give dig mulighed for at påminde den underskriftsbemyndigede for it-systemudbyderen.

6

Tilføj en Teknisk administrator. it-systemet er oprettet og du vil se detaljer for it-systemet.

Tilføj teknisk administrator

For at komme videre i processen er det vigtigt, at der tilknyttes en Teknisk administrator til systemet, som har til opgave at indsætte metadata og rapportere omkringsystemtests. Gå til afsnit 6.5 for tilføjelse af tekniskadministrator.

Funktionen er tilgængelig for rollerne:

- Administrator for it-udbyder

6.5 Tilføj en teknisk administrator

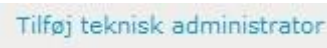
1

Vælg et it-system. Åbn detaljer for et it-system, som der ønskes tilføjet en Teknisk administrator til.

Biblioteks system

2

Tilføj Teknisk administrator. Klik på 'Tilføj teknisk administrator' i opgavemenuen 'Løs opgaver' til venstre.

Tilføj teknisk administrator

3

Vælg medarbejder fra liste

En liste over alle medarbejdere, der har været logget ind med deres medarbejdercertifikat fra din organisation, vil først blive vist. Du kan nu vælge en medarbejder og trykke på "næste" eller du kan vælge at trykke på "Tilføj Teknisk administrator manuelt".

Eller du kan vælge

Indtast eller rediger personoplysninger. CVR- nummer for organisationen vil være udfyldt automatisk og kan ikke redigeres. Hvis du har valgt manuelt at tilføje en Teknisk administrator, skal du indtaste brugerens navn, e-mail og RID-nummer (medarbejdernummer)



The screenshot shows a form with four input fields. The first field is labeled 'CVR-nummer*' and is empty. The second field is labeled 'Fulde navn*' and is empty. The third field is labeled 'E-mail*' and is empty. The fourth field is labeled 'RID-nummer er det unikke me' and is empty. A yellow question mark icon is visible to the right of the fourth field.

4

Tilføj Teknisk administrator. Klik på 'Tilføj' for at tilføje brugeren.



A rectangular button with the text 'Tilføj' in a sans-serif font.

5

Gå tilbage eller tilføj flere brugere. Du kan vælge at tilføje flere administratorer med det samme eller gå tilbage til listen med organisationer ved at klikke på 'Gå tilbage til it-systemet'.

Funktionen er tilgængelig for rollerne:

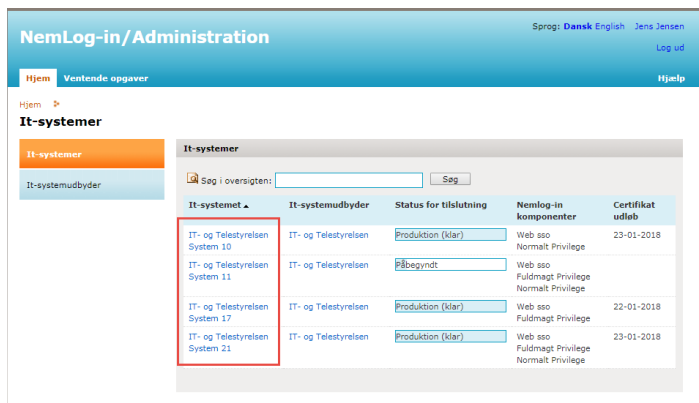
- Administrator for it-systemudbyder
- Administrator for it-leverandør

6.6 Fjern en teknisk administrator

Når du fjerner en Teknisk administrator vil brugeren ikke længere have administratorprivilegier for det pågældende it-system.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



2

Se administratorer. Se tekniske administratorer er under fanebladet 'Teknisk administrator'. Her ses it-systemets tilknyttede tekniske administratorer.

Teknisk administrator

3

Fjern teknisk administrator. Klik på 'Fjern' til højre for den tekniske administrator, som du ønsker at fjerne administratorprivilegier for.

4

Bekræft fjernelse. Klik på 'OK' for at bekræfte, at den tekniske administrator fjernes fra organisationen.

Funktionen er tilgængelig for rollerne:

- Administrator for it- systemudbyder
- Administrator for it-leverandør.

6.7 Slet it-system

Bemærk at sletning kun bør udføres, hvis it-systemet oprettes ved en fejl, da det ikke er muligt at fortryde en sletning.

1

Vælg et it-system. Åbn detaljer for et it-system ved at klikke på systemnavnet.



2

Slet it-system. Vælg 'Slet it-systemet' i opgavemenuen 'Løs opgaver' til venstre.



3

Bekræft sletning.

BEMÆRK! Sletning af it-systemet kan ikke fortrydes. Metadata og alle indstillinger for administratorer kan ikke genskabes. Fuldmagtsprivilegier (hvis nogen) vil også blive inddraget. Handlingen bør kun udføres, hvis it-systemet er oprettet ved fejl, it-systemet skal nedlægges eller ved grov vilkårsovertrædelse fra it-systemudbyder eller it-leverandørens side.

Marker checkboksen ud for 'Jeg har læst ovenstående og ønsker at slette it-systemet'.

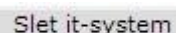


4

Slet it-systemet endeligt. Klik på 'Slet it-system'.

5

Gå tilbage til overbliksside
[Navnet på it-system] er nu slettet. Klik på 'Gå tilbage til oversigten'.



Funktionen er tilgængelig for rollerne:

- Administrator for it-systemudbyder

6.8 Tilføj en it-leverandør

Det er muligt at uddelegere den tekniske tilslutning af et it-system til en ekstern virksomhed. Dette gøres ved at 'tilføje en ny it-leverandør' til et it-system i NemLog-in /Administration.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



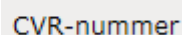
2

Tilføj it-leverandør. Klik på 'Tilføj ny it-leverandør' i menuen 'Løs opgaver' til venstre.



3

Angiv CVR-nummer. Indtast CVR-nummeret for it-leverandøren.



4

Tilføj. Klik på 'Tilføj valgte it-leverandør'

5

Se it-leverandører. Den valgte virksomhed vil nu have mulighed for at administrere it-systemet. Der vil blive afsendt en e-mail med instruktioner til virksomheden.

Klik på fanebladet 'it-leverandør' for at se alle virksomheder, som teknisk administration for it-systemet er uddelegeret til

Funktionen er tilgængelig for rollerne:

- Administrator for it-systemudbyder

6.9 Fjern en it-leverandør

Hvis en virksomhed ikke længere skal foretage den tekniske administration af en it- løsning, er det muligt for Administratoren for it-systemudbyder at fjerne virksomheden.

BEMÆRK!

Sletning af en it-leverandør kan ikke fortrydes og it-leverandøren vil ikke længere stå for den tekniske registrering af it-systemet. Bindinger til administratorer kan ikke genskabes og skal genopbygges manuelt, hvis virksomheden på et senere tidspunkt, skal stå for den tekniske administration igen.

1

Vælg et it-system. Åbn detaljer for et it-system ved at klikke på systemnavnet.

2

Se it-leverandører. Klik på fanebladet 'it-leverandør' for at se alle virksomheder, som teknisk administration for it-systemet er uddelegeret til.

3

Fjern. Klik på 'Fjern' ud for den it-leverandør, som ønskes fjernet fra it-systemet.

4

OK. Klik på 'OK'

Funktionen er tilgængelig for rollerne:

- Administrator for it-systemudbyder

7 Teknisk tilslutning af it-system

Den tekniske tilslutning af it-systemet, herunder håndtering af de tekniske data, udføres af en teknisk administrator. Den tekniske administrator kan enten være medarbejder i myndigheden, som udbyder it-systemet (it-systemudbyder) eller en medarbejder hos it-leverandøren, som har fået til opgave at stå for den tekniske tilslutning på myndighedens vegne (it-leverandøren).

7.1 Se it-systemets tekniske data

1

Vælg et it-system. Åbn detaljer for et it-system ved at klikke på systemnavnet.

2

For at foretage den tekniske tilslutning klik på fanen Integration eller Produktion

3

Se detaljer. it-systemets tekniske data vises. Det første område af skærbilledet, som har

it-systemets navn som overskrift, fx

'CSS Administration it-system', indeholder de primære tekniske oplysninger. Her finder du følgende oplysninger:

CSS Administration it-system

For Produktion

Entity ID, som bliver hentet fra metadatafilen.

Signeringscertifikat, som bliver hentet fra metadatafilen.

Krypteringscertifikat, som bliver hentet fra metadatafilen.-
Dato for Produktion. Her planlægges det hvornår it-systemet overgår til produktionsmiljøet.

Versioner af metadata registreret i NemLog-in. Bemærk, at der kan være flere versioner af metadata registreret, men kun én må være i produktion.

Nemlog-in komponenter. Om it-systemet benytter Signeringstjeneste.

Angivelse af hvordan fuldmagtsprivilegier skal udstedes (vises kun hvis it-systemet indeholder fuldmagtsprivilegier)

Integration Produktion

EntityID hentet fra metadatafilen. ?
https://saml.it21.dnz.test

Signeringscertifikat hentet fra metadatafilen
Udløbsdato 22-01-2018 ?

Krypteringscertifikat hentet fra metadatafilen
Udløbsdato 22-01-2018 ?

Produktion
12-02-2015 01:00:00

Versioner af metadata registreret i NemLog-in
1

NemLog-in komponenter
☐ Signeringstjeneste

Angiv hvordan fuldmagtsprivilegier skal udstedes af NemLog-in
☒ Inkluder fuldmagtsprivilegier i SAML Assertion ?
☒ Tillad at fuldmagter hentes via NemLog-in's fuldmagts-web-service. Signeringscertifikatet fra metadata benyttes til at autentificere mod fuldmagtserven. ?

Status for tilslutning

1 2 3 4

Forbered produktionsmiljø	Ansvarlig
1 Påbegyndt	Teknisk administrator
2 Produktion (ansøgt)	Teknisk administrator
3 Produktion (godkendt)	Administrator for it-systemudbyder
4 Produktion (klar)	

Status for tilslutning af it-systemet. Under 'Status for tilslutning' kan du se en illustration af, hvor langt it-systemet er i tilslutningsprocessen og nedenunder kan du se en detaljeret beskrivelse af de forskellige trin i tilslutningsprocessen.

Udvidet NemLog-in indstillinger, som angiver om it-systemet tillader simulerede MOCES login (NemLog-in Privat til Erhverv), og hvordan loginskærm i den forbindelse vises.

Udvidet NemLog-in indstillinger

☐ Tillad ikke at logge på med privat NemID på vegne af en virksomhed ?

Vælg den fortrukne visning for login grænsefladen ?
Borgerrettet visning

For Integration:

Entity ID, som bliver hentet fra metadatafilen.

Signeringscertifikat, som bliver hentet fra metadatafilen.

Krypteringscertifikat, som bliver hentet fra metadatafilen

Nemlog-in komponenter. Om it-systemet benytter Signeringstjeneste.

Angivelse af hvordan fuldmagtsprivilegier skal udstedes (vises kun hvis it-systemet indeholder fuldmagtsprivilegier).

Udvidet NemLog-in indstillinger, som angiver om it-systemet tillader simulerede MOCES login (NemLog-in Privat til Erhverv), og hvordan loginskærm i den forbindelse vises.

Status for tilslutning af it-systemet. Under 'Status for tilslutning' kan du se en illustration af, hvor langt it-systemet er i tilslutningsprocessen og nedenunder kan du se en detaljeret beskrivelse af de forskellige trin i tilslutningsprocessen.

Status for tilslutning

1	2	3	4
Forbered integrationstest	Ansvarlig		
1 Påbegyndt	Teknisk administrator		
Udfør integrationstest			
2 Integration test (klar)	Teknisk administrator		
3 Integration test (gennemført)	Teknisk administrator		
4 Integration test (godkendt)	NemLog-in Support		

Seneste provisionering af metadata:

4

Avanceret. I området 'Avanceret' nederst på siden er det muligt at se detaljeret lister over it-systemets:

- Attributter
- Privilegier
- Endpoints
- Metadataversioner (kun Produktion)
- Testbrugere (kun Integration)

5

Metadataversioner (kun produktion).

Under fanen 'Metadataversioner' kan man se tidligere versioner af uploadet metadata

samt dato for oprettelse i produktionsmiljøet.

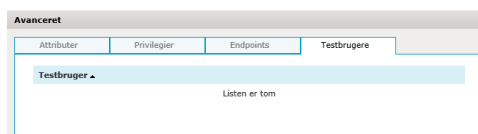
Avanceret

Attributter	Privilegier	Endpoints	Metadataver...
Versioner af metadata registreret i NemLog-in	Miljø/Tilstand	Status for tilslutning	Dato for oprettelse i produktionsmiljø
1	Produktion (klar)	Produktion	12-02-2015

6

Testbrugere (kun Integration).

Under fanen Testbrugere kan man se de testbrugere, som er oprettet for it-systemet. Hvis ikke der er testbrugere gøres der opmærksom på at Listen er tom.



Funktionen er tilgængelig for rollerne:

- Teknisk administrator

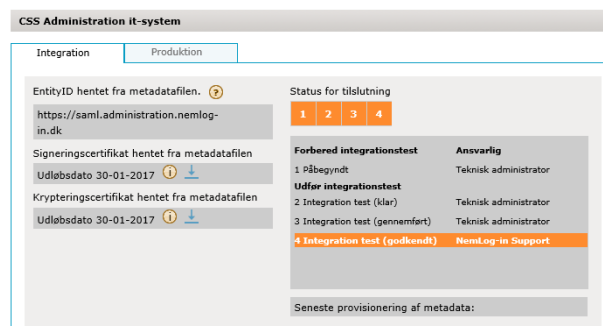
7.2 Rediger tekniske oplysninger om it-systemet

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. klik på fanen 'Integration' eller 'Produktion', alt efter hvilket miljø der skal ændres.



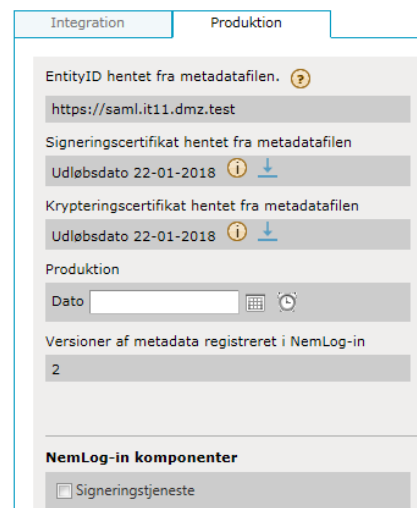
3

Ret eller indsæt detaljer. it-systemets tekniske data vises.

I det første område af skærbilledet, som har it-systemets navn som overskrift, fx 'CSS Administration it-system', har du mulighed for at rette følgende oplysninger:

- Produktionsdato (kun Produktion)
- Understøttelse af signeringstjeneste

Du kan indsætte eller rette de ønskede oplysninger.



4

Angiv hvordan fuldmagtsprivilegier skal udstedes af Nemlog-in. Denne indstilling vil kun være tilgængelig hvis it-systemet har fået tilføjet et fuldmagtsprivilegie.

Inkludér fuldmagtsprivilegier igennem SAML assertion

Tillad at fuldmagter hentes via NemLog-in fuldmagts-web-service

Der skal vælges minimum én måde man ønsker at udstede fuldmagtsprivilegier på.

Angiv hvordan fuldmagtsprivilegier skal udstedes af NemLog-in

- ☐ Inkludér fuldmagtsprivilegier i SAML Assertion ?
- ☐ Tillad at fuldmagter hentes via NemLog-in's fuldmagts-web-service. Signeringscertifikatet fra metadata benyttes til at autentificere mod fuldmagtserven. ?

5

Udvidede NemLog-in indstillinger

Borgere, som er fuldt ud tegningsberettigede for en virksomhed, har mulighed for at logge ind på vegne af virksomheden i it-systemer der benytter NemLog-ins Web-SSO løsning (for mere information og tekniske krav til fx metadatafilen, se Digitaliseringsstyrelsens site og dokumentation til NemLog-in Privat til Erhverv).

Under punktet 'Udvidet NemLog-in indstillinger skal du tage stilling til følgende:

- Om it-systemet skal tilbyde simuleret MOCES login.
- Henvender it-systemet sig primært til private borgere eller til virksomheder. Dette styrer det grafiske look for login-siden.

Bemærk: Hvis en borger allerede har en aktiv session med Nemlog-In, hvor vedkommende er logget ind på vegne af sin virksomhed, så vil der ske et Simuleret Medarbejder single sign-on (SSO) til tjenesteudbyderens it-system, uagtet at der er flueben i 'Tillad ikke at logge på med privat NemID på vegne af en virksomhed.'

Udvidet NemLog-in indstillinger

☐ Tillad ikke at logge på med privat NemID på vegne af en virksomhed ?

Vælg den fortrukne visning for login grænsefladen ?

Borgerrettet visning
Borgerrettet visning
Virksomhedsrettet visning

Gem tekniske oplysninger

6

Gem ændringer. Klik på 'Gem tekniske oplysninger' for at gemme ændringer.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.3 Administrer adgang til fuldmagtstjeneste

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration eller produktion alt efter hvor ændringerne ønskes foretaget.

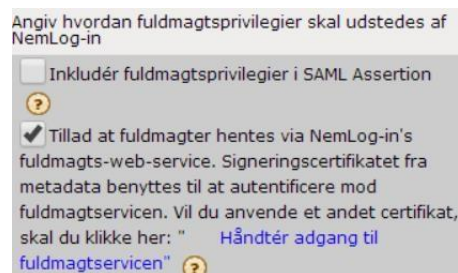


3

Håndtér adgang til fuldmagtsservicen.

I sektionen 'Angiv hvordan fuldmagtsprivilegier skal udstedes af Nemlog-in, klik på linket 'Håndtér adgang til fuldmagtsservicen'.

Linket vil kun være aktivt hvis man tidligere har valgt og gemt indstilling om at fuldmagter hentes via NemLog-in fuldmagt-web-service.



4

Administrer adgang til fuldmagtstjeneste.

Inkludér fuldmagtsprivilegier igennem SAML assertion

- Benyt servicens signeringscertifikat
- Angiv certifikat til integrationstest
- Angiv certifikat til produktion

Hvis flueben fjernes i 'Benyt servicens signeringscertifikat' skal der angives et unikt base64 encoded VOCES eller FOCES certifikat i Begge felter. Det skal være et test certifikat til integrationstest og et produktionscertifikat til produktion.



5

Gem ændringer. Klik på 'Gem' for at gemme ændringer.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.4 Tilføj et nyt privilegie

Her kan du registrere et nyt privilegie for it-systemet, som skal kunne tildeles i NemLog-in Brugeradministration.

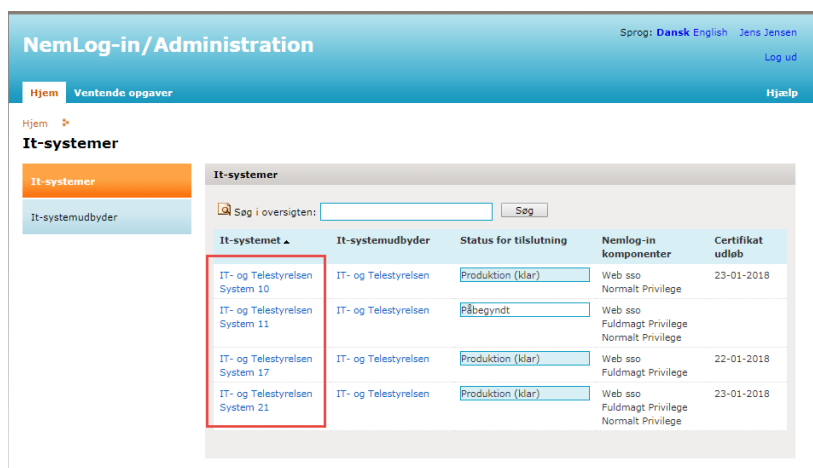
BEMÆRK!

Det er ikke muligt at tilføje et privilegie, når it-systemet har følgende status:

- Integration test (ansøgt)
- Produktion (ansøgt)
- Produktion (godkendt)
- Produktion (klar).

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



2

Teknisk administration. Klik på fanen Integration eller Produktion alt efter hvilket miljø privilegierne skal tilføjes.



3

Tilføj privilegie. Klik på 'Tilføj privilegie' i menuen 'Løs opgaver' til venstre.

4

Indsæt oplysninger. Indtast oplysninger for privilegiet i formularen, som bliver synligt for brugerne. Du skal angive følgende oplysninger:

- Privilegienavn
- Engelsk navn
- Privilegie
- Om det er et Medarbejder privilegie eller et Borger fuldmagtsprivilegie
- Kort beskrivelse (fx hvad slutbrugerne kan benytte privilegiet til).

Hvis der ikke er tale om et rent testsystem, er det vigtigt, at navne på privilegier samt dansk og engelsk beskrivelse er præcise, da både navn på privilegie og beskrivelserne senere kan ses af brugerne.

Vær opmærksom på, at et almindeligt privilegie er rettet mod medarbejdere og skal gives igennem Brugeradministrationsportalen, når systemet er i Produktion (hvor det skal indgå i en eller flere rettigheder). Et fuldmagtsprivilegie er rettet mod borgere og vil blive givet igennem Fuldmagtsportalen, når et system er i produktion.

5

Tilføj privilegie. Klik på 'Tilføj privilegie'.

6

Gå tilbage og se oplysninger. Når ønskede privilegier er oprettet, kan der navigeres tilbage til siden med tekniske oplysninger ved at klikke 'Gå tilbage til tekniske oplysninger om it-systemet' i den gule informationsboks øverst på siden.

7

Se privilegier. Klik på fanebladet 'Privilegier' under 'Avanceret' nederst på siden for at se oprettede privilegier for it-systemet.

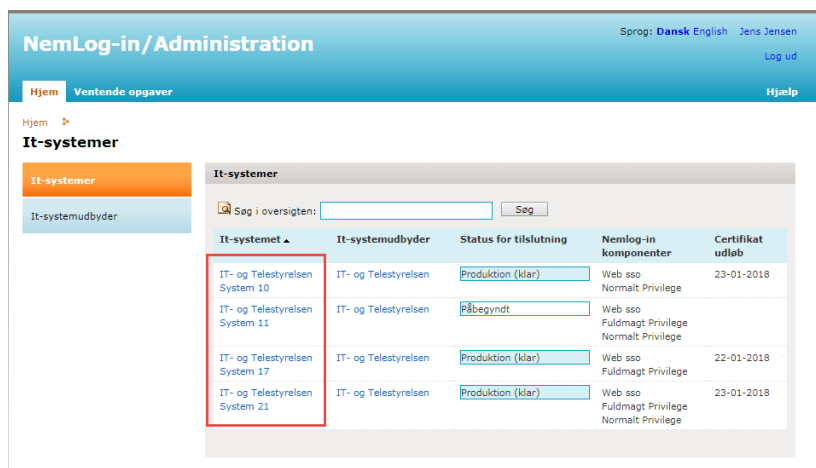
Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.5 Opatér privilegie

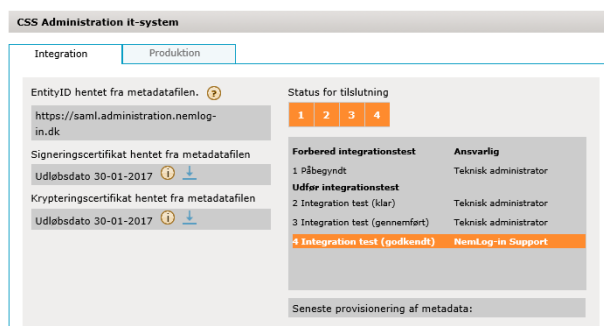
1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



2

Teknisk administration. klik på fanen 'Integration' eller 'Produktion', alt efter miljø privilegierne skal tilføjes.



3

Se privilegier. Klik på fanebladet 'Privilegier' under 'Avanceret' nederst på siden for at se oprettede privilegier for it-systemet.

4

Åbn privilegie. Vælg et privilegie i listen ved at klikke på privilegienavnet.

5

Ret oplysninger. Indsæt eller ret oplysninger i formularen.

6

Gem. Klik på 'Gem privilegieændringer'

Bemærk!

Ændringen træder først i kraft i testmiljøet efter du igen anmoder om integrationstest, og vil først være aktiv i produktion efter, at den nye version er i status

"Produktion (klar)".

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.6 Fjern privilegie

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration eller Produktion alt efter i hvilket miljø privilegierne skal fjernes.

3

Se privilegier. Klik på fanebladet 'Privilegier' under 'Avanceret' nederst på siden for at se oprettede privilegier for it-systemet.

4

Find privilegie. Vælg et privilegie i listen ved at klikke på privilegienavnet.

5

Fjern. Klik på 'Fjern privilegie'.

6

Bekræft. Klik på 'OK' for at bekræfte at privilegiet skal fjernes.

Bemærk!

Ændringen træder først i kraft i testmiljøet efter du igen anmoder om integrationstest, og vil først blive fjernet i produktion efter, at den nye version er i status "Produktion (klar)".

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.7 Indlæs tekniske data (metadatafil)

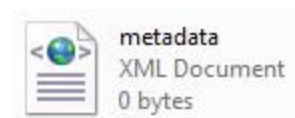
1 Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2 Teknisk administration. Klik på fanen Integration eller Produktion alt efter i hvilket miljø der arbejdes i.

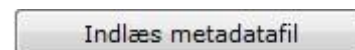
3 Indlæs. Klik på 'Indlæs metadatafil' i menuen 'Løs opgaver' til venstre. Dette er kun muligt i Produktion hvis man er i gang med tilslutning Af nyt system.

4 Gennemse. Klik på 'Vælg fil'.

5 Vælg fil. Find den passende metadatafil (XML-format) lokalt på din computer og klik på 'Open'.



6 Indlæs. Stinavnet på filen vil fremgå af tekstfeltet. Klik på 'Indlæs metadatafil'.



Bemærk!

Filen vil automatisk blive kontrolleret af NemLog-in metadatavalidator inden den indlæses. Hvis validatoren finder fejl i metadatafilen, gøres der opmærksom herom og det er ikke muligt at indlæse filen.

Når fejlbeskeden vises, vil det være muligt at se hvilke fejl metadatavalidatoren har fundet ved at klikke 'Fejl liste'.

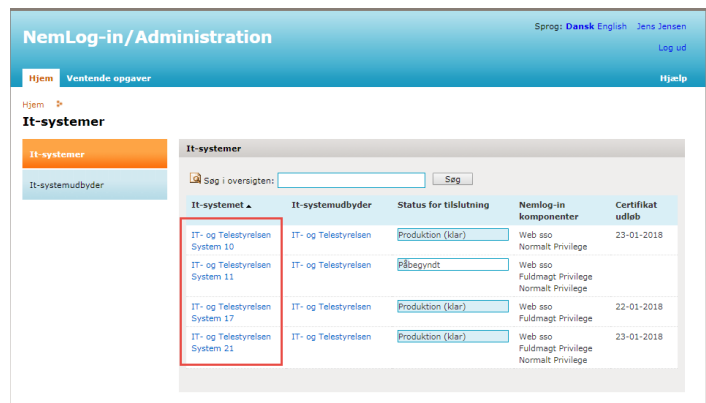
Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.8 Download NemLog-in metadata

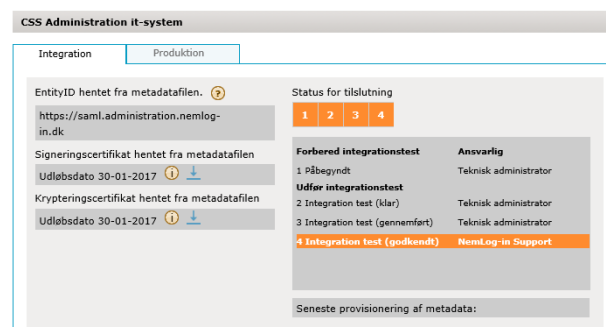
1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



2

Teknisk administration. Klik på fanen Integration eller Produktion alt efter i hvilket miljø der arbejdes i.



3

Download. Klik på 'Download NemLog-in metadata' i menuen 'Løs opgaver' til venstre for at downloade metadatafilen på din computer.

Download NemLog-in metadata

4

Hent fil. Klik på linket for at hente NemLog-in metadatafil.

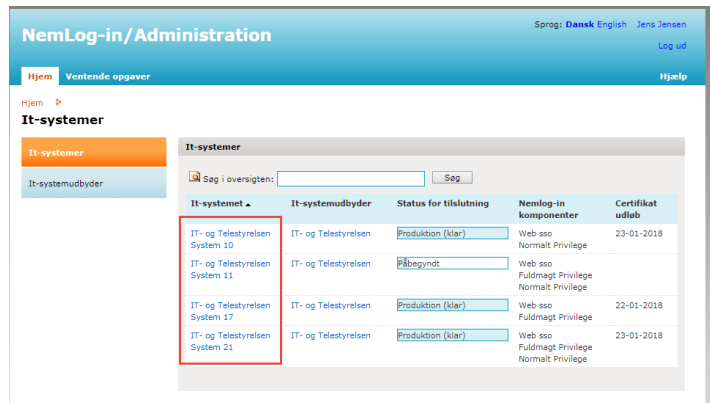
Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.9 Validér tekniske data (metadata)

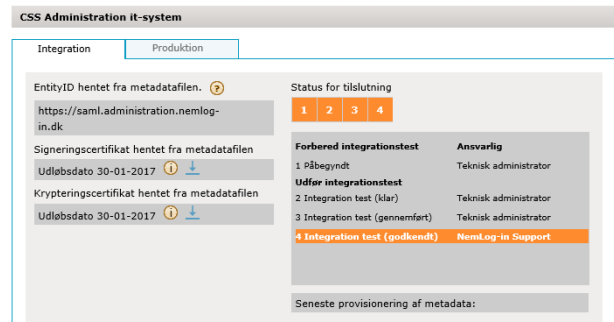
1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



2

Teknisk administration. Klik på fanen Integration eller Produktion alt efter i hvilket miljø der arbejdes i.



3

Validér. Klik på 'Valider' i menuen 'Løs opgaver' til venstre. Dette er kun muligt i produktion hvis man er i gang med tilslutning af ny version af systemet.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

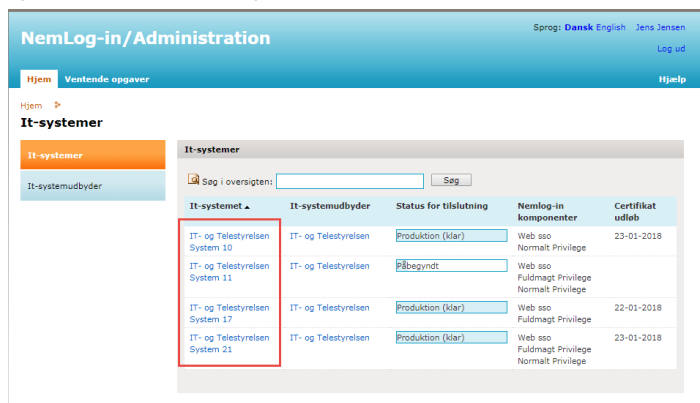
7.10 Se versioner af teknisk data (metadata) – kun produktion

Hvis et it-system i produktion skal opdateres, vil metadata typisk også skulle opdateres.

Derfor er det muligt i NemLog-in Administration at oprette nye metadataversioner for it-systemet. Det er her også muligt at se tidligere versioner.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



2

Liste af versioner. Klik på fanebladet "metadataversioner".

Avanceret			
Attributer	Privilegier	Endpoints	Metadataver...
Versioner af metadata registreret i NemLog-in		Miljø/Tilstand	Status for tilslutning
3	Påbegyndt	Påbegyndt	
2	Produktion (klar)	Produktion	26-06-2017
1	Produktion (klar)	Udfaset	12-02-2015

3

Åbn en version. Listen med versioner af metadata vises.

I oversigten vises følgende oplysninger:

- Versioner af metadata registreret i NemLog-in.
- Miljø/Tilstand.
- Status for tilslutning af it-systemet.
- Dato for oprettelse af produktionsmiljø.

Det er muligt at åbne en version ved at klikke på versionsnummeret.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

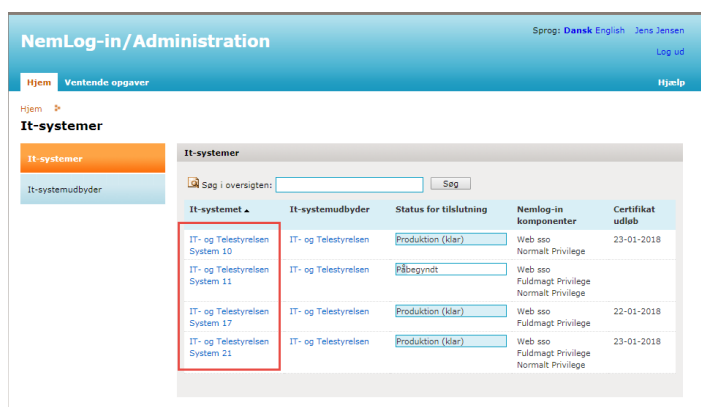
7.11 Opret en ny version af teknisk data (metadata)

Hvis et it-system i produktion skal opdateres, vil metadata også typisk skulle opdateres.

Derfor er det muligt i Administrationen at oprette nye versioner af de tekniske data. Det er her også muligt at se tidligere versioner.

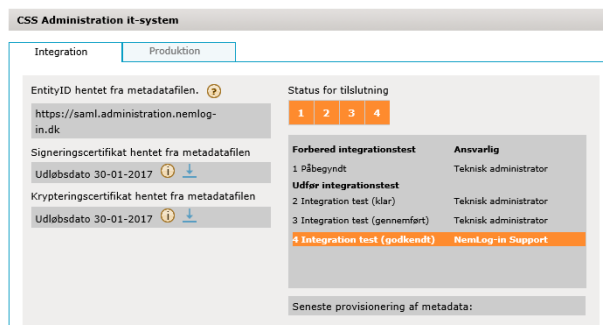
1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



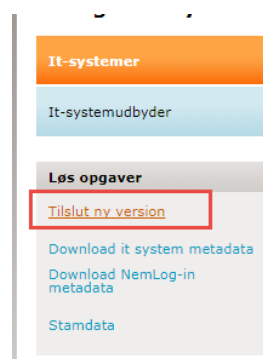
2

Teknisk administration. Klik på fanen Integration eller Produktion alt efter i hvilket miljø der arbejdes i.



3

Tilslut ny version. Klik på 'Tilslut ny version' i menuen 'Løs opgaver' til venstre.



4

Opret version. Vælg, om du vil kopiere de nuværende metadata over i den nye version ved at sætte hak i 'Kopier metadata for nuværende version til den nye version'. Klik på 'Opret'.

Ny version it-system

Ny version it-system

En ny version indeholder metadata for den kommende version af it-systemet.
Du kan vælge at kopiere de nuværende metadata over i den nye version.

☐ Kopier metadata for nuværende version til den nye version

< Tilbage

Opret

5

Udfyld information. Udfyld de relevante data, herunder:

Produktion (produktionsdato)

6

Klik på 'Gem tekniske oplysninger'.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.12 Tilføj en NemID borgertestbruger

Borgertestbrugere kan kun tilføjes hvis it-systemet indeholder et eller flere fuldmagtsprivilegier.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

Sprog: Dansk English Jens Jensen

Log ud

Hjem

Ventende opgaver

Hjælp

Hjem >

It-systemer

It-systemer

It-systemudbyder

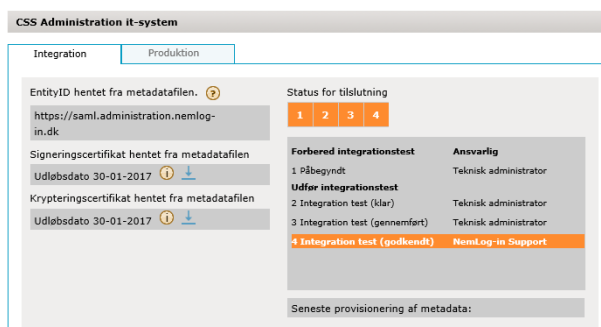
Søg i oversigten:

Sej

It-systemet	It-systemudbyder	Status for tilslutning	Nemlog-in komponenter	Certifikat udløb
IT- og Telestyrelsen System 10	IT- og Telestyrelsen	Produktion (klar)	Web sso Normalt Privilege	23-01-2018
IT- og Telestyrelsen System 11	IT- og Telestyrelsen	Påbegyndt	Web sso Fuldmagt Privilege Normalt Privilege	
IT- og Telestyrelsen System 17	IT- og Telestyrelsen	Produktion (klar)	Web sso Fuldmagt Privilege	22-01-2018
IT- og Telestyrelsen System 21	IT- og Telestyrelsen	Produktion (klar)	Web sso Fuldmagt Privilege Normalt Privilege	23-01-2018

2

Teknisk administration. Klik på fanen Integration.



3

Tilføj. Klik på 'Tilføj Borger-testbruger'.



4

Vælg Login type

Vælg login-typen NemID for den testbruger, der skal oprettes

5

Indtast oplysninger om testbrugeren.

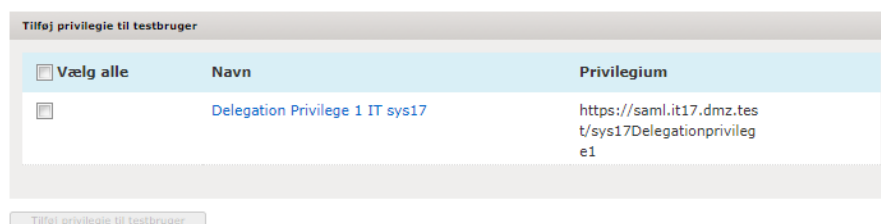
Indtast oplysninger om testbrugeren i formularen.

Du skal indtaste navn, PID- & CPR-nummer.

6

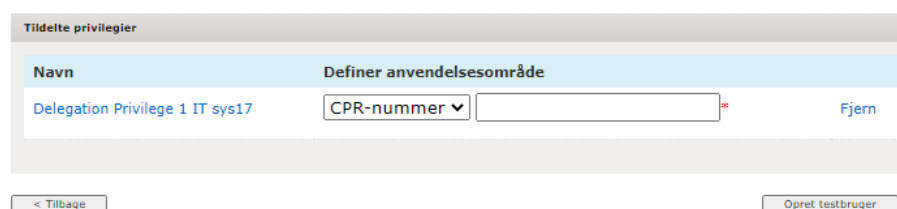
Tilføj fuldmagtsprivilegier til bruger.

Markér de privilegier i listen, som skal tilføjes til brugeren.



Klik på 'Tilføj privilegie til testbruger'.

De tilføjede privilegier vil fremgå i oversigten 'Tildelte privilegier'.



For at fjerne et privilegie fra testbrugeren, klikkes 'Fjern' ud for privilegiet i oversigten.

7

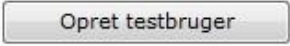
Sæt begrænsninger for privilegiet. Du kan begrænse privilegiets gyldighedsområde ved at klikke på rullemenuen med mærkatet 'CPR-nummer'.

Du kan begrænse privilegiet til at gælde til et specifikt CPR-nummer ved at indtaste CPR-nummeret til højre for rullemenuen i tekstfeltet.

Når du sætter en begrænsning, så gælder privilegiet kun for det angivne CPR-nummer.

8

Opret. Klik på 'Opret testbruger'

A rectangular button with a light gray background and a thin border, containing the text 'Opret testbruger'.

Funktionen er tilgængelig for rollerne:

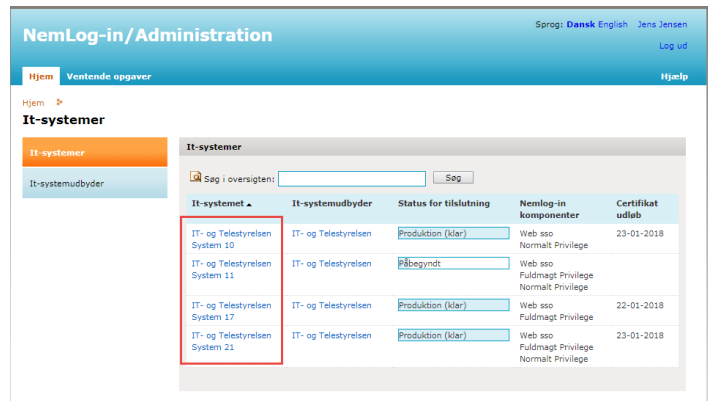
- Teknisk administrator

7.13 Tilføj en MitID borgertestbruger

Borgertestbrugere kan kun tilføjes hvis it-systemet indeholder et eller flere fuldmagtsprivilegier.

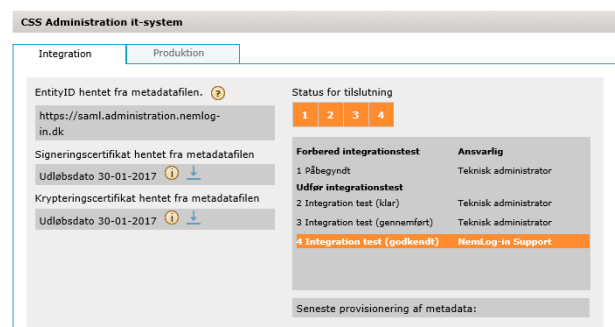
1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.



2

Teknisk administration. Klik på fanen Integration.



3

Tilføj. Klik på 'Tilføj Borger-testbruger'.



4

Vælg Login type

Vælg login-typen MitID for den testbruger, der skal oprettes.

Oprettelse af testbruger

Login type ☐ Nem ID ☒ Mit ID

Brugernavn*

5

Indtast oplysninger om testbrugeren.

Indtast oplysninger om testbrugeren formularen.

Du skal indtaste brugernavn.

6

Tilføj fuldmagtsprivilegier til bruger.

Markér de privilegier i listen, som skal tilføjes til brugeren.

Vælg alle	Navn	Privilegium
☐	Delegation Privilege 1 IT sys17	https://saml.it17.dmz.test/sys17Delegationprivilege1

Tilføj privilegie til testbruger

Klik på 'Tilføj privilegie til testbruger'.

De tilføjede privilegier vil fremgå i oversigten 'Tildelte privilegier'.

Navn	Definer anvendelsesområde
Delegation Privilege 1 IT sys17	CPR-nummer Fjern

< Tilbage Opret testbruger

For at fjerne et privilegie fra testbrugeren, klikkes 'Fjern' ud for privilegiet i oversigten.

7

Sæt begrænsninger for privilegiet. Du kan begrænse privilegiets gyldighedsområde ved at klikke på rullemenuen med mærkatet 'CPR-nummer'.

Du kan begrænse privilegiet til at gælde til et specifikt CPR-nummer ved at indtaste CPR-nummeret til højre for rullemenuen i tekstfeltet.

Når du sætter en begrænsning, så gælder privilegiet kun for det angivne CPR- nummer.

8

Opret. Klik på 'Opret testbruger'

Opret testbruger

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.14 Tilføj en NemID medarbejdertestbruger

1

Vælg et it-system. Åbn detaljer for et it-system ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration

3

Tilføj. Klik på 'Tilføj Medarbejder-testbruger'.

4

Vælg Login type og Indtast oplysninger om bruger.

Vælg login-typen NemID for den testbruger, der skal oprettes.

Indtast oplysninger om testbrugeren i formularen.

Du skal angive:

- Navn
- CVR-nummer

Du kan også vælge at angive:

- RID-nummer
- P-enhed
- SE-nummer
- E-mail.

Tilføj privilegier til bruger. Markér de privilegier i listen, som skal tilføjes til

5

The screenshot shows the 'Tilføj privilegie til testbruger' (Add privilege to test user) interface. It consists of two main parts: a form for user details and a table for selecting privileges.

User Details Form:

- Login type: ☒ Nem ID ☐ Mit ID
- Navn*:
- CVR-nummer*:
- RID-nummer (medarbejdersnummer):
- P-enhed:
- SE-nummer:
- E-mail:

Privilege Selection Table:

☐ Vælg alle	Navn	Privilegium
☒	Delegation Privilege 1 IT sys17	https://saml.it17.dmz.test/sys17Delegationprivilege1

At the bottom of the table is a button labeled 'Tilføj privilegie til testbruger'.

Klik på 'Tilføj privilegie til testbruger'. De tilføjede privilegier vil fremgå i oversigten 'Tildelte privilegier'.

Navn	Definer anvendelsesområde
Delegation Privilege 1 IT sys17	CPR-nummer

< Tilbage O

For at fjerne et privilegie fra testbrugeren igen, klikkes på 'Fjern' ud for privilegiet i oversigten.

6

Sæt begrænsninger for privilegiet. Du kan begrænse privilegiets gyldighedsområde ved at klikke på rullemenuen med mærkatet 'CVR-nummer'.

Du kan begrænse privilegiet til at gælde et

specifikt CVR-nummer, SE-nummer eller P-enhed. Vælg CVR-nummer, P-enhed eller på SE-nummer og indsæt dernæst nummeret til højre for rullemenuen i tekstfeltet.

Når du sætter en begrænsning, så gælder privilegiet kun for det angivne CVR-nummer, P-enhed eller SE-nummer.

7

Opret. Klik på 'Opret testbruger'.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.15 Tilføj en MitID medarbejdertestbruger

1 **Vælg et it-system.** Åbn detaljer for et it-system ved at klikke på systemnavnet.

2 **Teknisk administration.** Klik på fanen Integration

3 **Tilføj.** Klik på 'Tilføj Medarbejder-testbruger'.

4 **Vælg Login type og Indtast oplysninger om bruger.**
Vælg login-typen MitID for den testbruger, der skal oprettes.
Indtast oplysninger om testbrugeren i formularen.

Du skal angive:

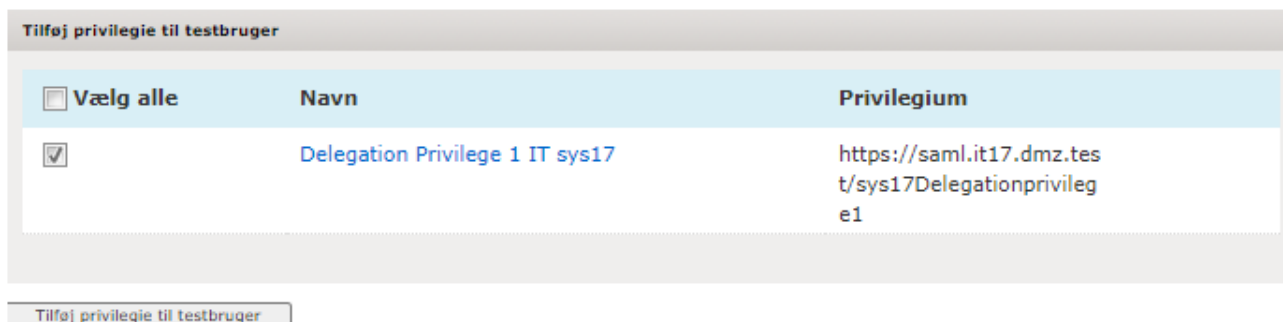
- IAL (Identification Assurance Level)
- Navn
- CVR-nummer

Du kan også vælge at angive:

- RID-nummer.
- P-enhed
- SE-nummer
- E-mail.



5 **Tilføj privilegier til bruger.** Markér de privilegier i listen, som skal tilføjes til brugeren.



☐ Vælg alle	Navn	Privilegium
☒	Delegation Privilege 1 IT sys17	https://saml.it17.dmz.test/sys17Delegationprivilege1

Klik på **'Tilføj privilegie til testbruger'**. De tilføjede privilegier vil fremgå i oversigten **'Tildelte privilegier'**.

Navn	Definer anvendelsesområde
Delegation Privilege 1 IT sys17	CPR-nummer *

< Tilbage Opret testbruger

For at fjerne et privilegie fra testbrugeren igen, klikkes på **'Fjern'** ud for privilegiet i oversigten.

6

Sæt begrænsninger for privilegiet. Du kan begrænse privilegiets gyldighedsområde ved at klikke på rullemenuen med mærkatet **'CVR-nummer'**.

Du kan begrænse privilegiet til at gælde et specifikt CVR-nummer, SE-nummer eller P-enhed. Vælg CVR-nummer, P-enhed eller på SE-nummer og indsæt dernæst nummeret til højre for rullemenuen i tekstfeltet.

Når du sætter en begrænsning, så gælder privilegiet kun for det angivne CVR-nummer, P- enhed eller SE-nummer.

7

Opret. Klik på **'Opret testbruger'**.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

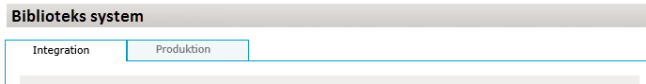
7.16 Opdater privilegier for eksisterende borgertestbruger

1

Vælg et it-system. Åbn detaljer for it- systemet ved at klikke på systemnavnet.

2

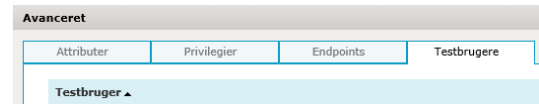
Teknisk administration. Klik på fanen Integration



3

Find testbruger. Scroll ned på siden og find fanen 'Testbrugere'.

Klik på navnet på den testbruger i oversigten, som du ønsker ændret.



4

Ændring af privilegier. Hvis du vil ændre brugerens privilegier, er fremgangsmåden den samme som ved oprettelse. Se afsnit 7.12 og 7.13. Credential type, samt brugeroplysninger, bortset fra privilegier, kan ikke ændres.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

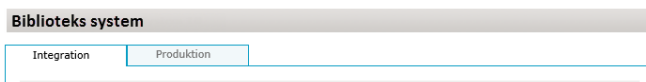
7.17 Opdater eksisterende medarbejdertestbruger

1

Vælg et it-system. Åbn detaljer for it- systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration



3

Find testbruger. Scroll ned på siden og find fanen 'Testbrugere'.

Klik på navnet på den testbruger i oversigten, som du ønsker ændret.

4

Ændring af brugeroplysninger. Hvis du vil ændre brugerens oplysninger, er fremgangsmåden den samme som ved oprettelse. Se afsnit 7.14 og 7.15. Credential type, samt Brugernavn, kan ikke ændres.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

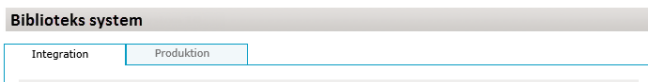
7.18 Fjern en testbruger

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration



3

Find testbruger. Scroll ned på siden og find fanen 'Testbrugere'.

Klik på 'Fjern' ud for testbrugeren i oversigten, du ønsker ændret.

4

Bekræft. Klik på 'OK' for at bekræfte.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.19 Indlæs testrapport

Testrapporten der skal indlæses er en rapport over den obligatoriske integrationstest der skal udføres på en ny tilslutning i overensstemmelse med digitaliseringsstyrelsens retningslinjer.

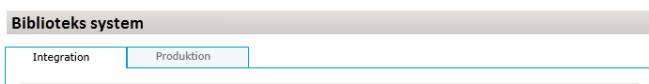
Test rapport kan kun indlæses i version 1 af et system når et system er i status "Integration test (klar)"

1

Vælg et it-system. Åbn detaljer for it- systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration



3

Indlæs testrapport. Klik på 'Indlæs testrapport' i menuen 'Løs opgaver' til venstre.

4

Indlæs testrapport fra integrationstesten.

Klik på 'Vælg fil' og vælg fil med udfyldt og underskrevet testrapport.

5

Indlæs testrapport. Klik på 'Indlæs testrapport' knappen for at bekræfte upload af valgte test rapport.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.20 Download testrapport

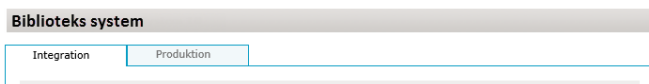
Testrapporten er en rapport over den integrationstest af it-systemet, som er blevet foretaget.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration



3

Download testrapport. Klik på 'Download testrapport' i menuen 'Løs opgaver' til venstre.

4

Åbn testrapport. Klik på 'Open' for at åbne rapporten.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.21 Ansøg om integrationstest

For at tilslutte et it-system til NemLog-in og for at komme i produktionsmiljøet, skal der i version 1 foretages en integrationstest, hvor der skal gennemføres en række testcases.

Før it-systemet kan flyttes til integrationstestmiljø, skal der ansøges om at kunne foretage en integrationstest. Bemærk, at metadata låses fast under testen og først kan ændres, når integrationstesten er udført.

Når din ansøgning er blevet godkendt af NemLog-in, modtager du en meddelelse samt en ny opgave under 'Ventende opgaver' og it-systemet flyttes til integrationstestmiljøet. Hvis din ansøgning bliver afvist, vil du også få en e-mail herom.

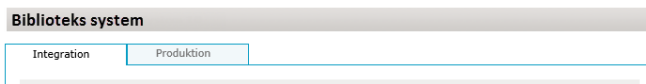
Hvis der bliver ansøgt om integrationstest fra en senere version end version 1, vil metadata og testdata blive overført automatisk til integrationstestmiljøet. Der vil her ikke være en efterfølgende godkendelsesproces og systemet bliver fastlåst.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration



3

Ansøg. Klik på 'Ansøg om integrationstest' menuen 'Løs opgaver' til venstre.

Bemærk!

Det er kun muligt at ansøge om at få et it-system i integrationstest, når it-systemet har status 'Påbegyndt'.

4

Anmod. Læs teksten inden du fortsætter. Klik dernæst på 'Anmod om integrationstest'.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.22 Anmod om overførsel til produktion

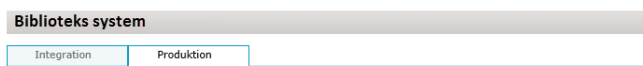
Når der er blevet gennemført en succesfuld integrationstest af it-systemet, kan du anmode om at få overført it-systemet til produktionsmiljøet.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Produktion



3

Ansøg. Klik på 'Ansøg om produktion' i menuen 'Løs opgaver' til venstre.

BEMÆRK!

Det er i version 1 af et system, kun muligt at ansøge om at få et it-system i produktionsmiljø, når it-systemets tekniske data har status 'Integration test (godkendt)'.

Så snart et system er i minimum version 2, kan du ansøge om at få en ny version i produktion. Vær opmærksom på, at det angivne produktionstidspunkt bestemmer

det præcise tidspunkt, hvor metadata tidligst kan træde i kraft. For at systemet går i produktion kræver det, at Administrator for

it-systemudbyder, NemLog-in leverandør, og i nogle tilfælde at NemLog-in administration har godkendt opgaver i forbindelse med ansøgning om produktion. Hvis disse opgaver ikke er godkendt på det angivne produktionstidspunkt, vil systemet ikke gå i produktion før efter at opgaverne faktisk er godkendt. Fra den sidste opgave er godkendt kan der gå op til 5 min. før den nye produktionsversion træder i kraft.

BEMÆRK!

It-systemet kan kun overføres til produktionsmiljøet, hvis gældende vilkår for it-systemudbyderen er underskrevet. Hvis der ikke er underskrevet gældende vilkår, vil du blive informeret om dette, og det vil ikke være muligt at anmode om overførsel til produktionsmiljø. Du har mulighed for at påminde den underskriftsbemyndigede for it-systemet om at underskrive vilkår.

4

Anmod. Læs teksten inden du fortsætter. Klik dernæst på 'Anmod om overførsel til produktion'.

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.23 Skift Certifikat

Det er muligt at opdatere signeringscertifikatet, krypteringscertifikatet og certifikatet til brug i fuldmagtstjenesten.

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Teknisk administration. Klik på fanen Integration eller Produktion, alt efter i hvilket miljø certifikatet skal udskiftes.

3

Skift certifikat. Klik på 'Skift certifikat' i menuen 'Løsopgaver' til venstre.

4

Åbn testrapport. Klik på 'Browse' ud for det certifikat der ønskes udskiftet.

Ud for krypteringscertifikatet og certifikatet til fuldmagtstjenesten er det muligt at benytte det samme certifikat som ved signeringstjenesten

ved at klikke i boksen 'Benyt servicens signeringscertifikat'

Administer udskiftning af certifikater

Udskift certifikater

Vælg det certifikat (CER-format), som du ønsker at indlæse i metadata

Udskift signeringscertifikat

Browse...

☐ Benyt servicens signeringscertifikat

Udskift krypteringscertifikat

Browse...

Vælg det certifikat (CER-format), som du ønsker at indlæse i fuldmagtstjenesten

☐ Benyt servicens signeringscertifikat

Udskift certifikat

Browse...

5

Godkend. Klik på Godkend udskiftning'

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.24 Opret ny systembruger

1

Vælg Brugerorganisationen hvor systembrugeren skal oprettes.

Brugerorganisation	CVR-nummer	Vilkår underskrevet	Oprettet
DRACHMANN ADVOKATER I/S	20841133	Tilsluttet	24-01-2013
INTECH ApS	24234738	Tilsluttet	24-01-2013
IT- og Telestyrelsen	26769388	Tilsluttet	17-09-2012
JENS YTZEN, SÆDDING A/S	26157447	Tilsluttet	19-03-2013
KNUD BAGER	11175384	Tilsluttet	24-01-2013
NNIT A/S	21093106	Tilsluttet	17-09-2012
Økonomistyrrelsen	10213231	Tilsluttet	17-09-2012

2

Vælg 'Tilføj systembruger' under 'løs opgaver' i menuen til venstre

Løs opgaver

- Tilføj administratorrollerne til en bruger
- Slet brugerorganisation
- Tilføj administrator for systembrugere
- Tilføj systembruger**

3

Udfyld Navn og entity id, og upload certifikater for signering. Bemærk at Entity ID skal starter med "https://wsc." og certifikatet skal være VOCES eller FOCES.

Tekniske oplysninger

Navn:

Beskrivelse:

Produktion

EntityId (Skal starte med https://wsc.):

Signeringscertifikat:

Vælg:

Næste signeringscertifikat (rullende skift):

Vælg:

Sidste provisioneringsdato for produktionsmiljø:

Integrationstest

EntityId (Skal starte med https://wsc.):

Signeringscertifikat:

Vælg:

Næste signeringscertifikat (rullende skift):

Vælg:

Sidste provisioneringsdato for integrationstestmiljø:

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.25 Vedligehold systembruger

1

Vælg Brugerorganisationen hvor systembrugeren skal vedligeholdes.

Brugerorganisation	CVR-nummer	Vilkår underskrevet	Oprettet
DRACHMANN ADVOKATER I/S	20841133	Tilsluttet	24-01-2013
INTECH ApS	24234738	Tilsluttet	24-01-2013
IT- og Telestyrelsen	26769388	Tilsluttet	17-09-2012
JENS YTZEN, SÆDDING A/S	26157447	Tilsluttet	19-03-2013
KNUD BAGER	11175384	Tilsluttet	24-01-2013
NNIT A/S	21093106	Tilsluttet	17-09-2012
Økonomistyrelsen	10213231	Tilsluttet	17-09-2012

2

Vælg fanen Systembruger og tryk på den systembruger der ønskes vedligeholdt

Navn	Entity Id	Oprettet
https://wsc.expiredOkonoFoces.env	https://wsc.expiredOkonoFoces.env	29.4.2015
https://wsc.expiredOkonoVoces.env	https://wsc.expiredOkonoVoces.env	29.4.2015
https://wsc.revokedOkonoFoces.env	https://wsc.revokedOkonoFoces.env	29.4.2015
https://wsc.revokedOkonoVoces.env	https://wsc.revokedOkonoVoces.env	29.4.2015
https://wsc.ServProvOkono1.env	https://wsc.ServProvOkono1.env	29.4.2015
https://wsc.UserOrgOkono1.env	https://wsc.UserOrgOkono1.env	29.4.2015

3

Ændr de ønskede oplysninger og tryk Gem tekniske oplysninger.

Tekniske oplysninger

Navn

Beskrivelse

Produktion

EntityId (Skal starte med https://wsc.)

Signeringscertifikat
SERIALNUMBER=CVR:21093106-FID:10155358 +
CN=KFOBS-TEST-FOCES-075 (funktionscertifikat),
O=NNIT A/S // CVR:21093106, C=DK

Vælg

Næste signeringscertifikat (rullende skift)
SERIALNUMBER=CVR:21093106-FID:10155358 +
CN=KFOBS-TEST-FOCES-075 (funktionscertifikat),
O=NNIT A/S // CVR:21093106, C=DK

Vælg

Sidste provisioneringsdato for produktionsmiljø
29-04-2015 04:11:31

[< Tilbage](#)

Integrationstest

EntityId (Skal starte med https://wsc.)

Signeringscertifikat
SERIALNUMBER=CVR:21093106-FID:10155358 +
CN=KFOBS-TEST-FOCES-075 (funktionscertifikat),
O=NNIT A/S // CVR:21093106, C=DK

Vælg

Næste signeringscertifikat (rullende skift)
SERIALNUMBER=CVR:21093106-FID:10155358 +
CN=KFOBS-TEST-FOCES-075 (funktionscertifikat),
O=NNIT A/S // CVR:21093106, C=DK

Vælg

Sidste provisioneringsdato for integrationstestmiljø
29-04-2015 04:11:31

[Gem tekniske oplysninger](#)

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.26 Provisioner systembruger til integrationstest

1

Gå til den ønskede systembruger (se 7.25 Vedligehold systembruger) og tryk på Provisioner til integrationstest i menuen Løs opgaver.

Når en teknisk administrator trykker på provisioner til integrationstest bliver systembrugeren provisioneret til NemLog-in Integrationstest miljøet. Der laves en validering på certifikatet og systembrugers metadata oprettes og provisioneres.

Løs opgaver

- [Provisioner til integrationstest](#)
- [Provisioner til produktion](#)
- [Skift system bruger ejer](#)
- [Anmod om web service adgang](#)

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.27 Provisioner systembruger til Produktion

1

Gå til den ønskede systembruger (se 7.25 Vedligehold systembruger) og tryk på Provisioner til produktion i menuen Løs opgaver.

Når en teknisk administrator trykker på provisioner til produktion bliver systembrugeren provisioneret til NemLog-in produktion. Der er ikke nogen godkendelse forbundet med at provisionere til produktion. Der laves en validering på certifikatet og systembrugers metadata oprettes og provisioneres.

Løs opgaver

[Provisioner til integrationstest](#)
[Provisioner til produktion](#)
[Skift system bruger ejer](#)
[Anmod om web service adgang](#)

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.28 Skift System Bruger Ejer

1

Gå til den ønskede systembruger (se 7.25 Vedligehold systembruger) og tryk på Skift system bruger ejer.

Løs opgaver

[Provisioner til integrationstest](#)
[Provisioner til produktion](#)
[Skift system bruger ejer](#)
[Anmod om web service adgang](#)

2

Indtast CVR nummer på den som er service aftager og tryk på Skift Service Aftager ejer knappen for at gemme ændringen.

Skift Service Aftager ejer**Ændre ejerskab af Service Aftager**

Her kan du ændre ejeren af Service Aftager

CVR number

< Tilbage

Skift Service Aftager ejer

3Funktionen er tilgængelig for rollerne:

- KFOBS administrator

7.29 Anmod om web service adgang

1

Gå til den ønskede systembruger (se 7.25 Vedligehold systembruger) og klik på 'Anmod om web service adgang'.

2

På oversigten over web service udbydere vælges den webservice hvor der ønskes adgang.

Web Service Udbydere		
Søg i oversigten: Søg		
Web service	Web service udbyder	Adgang til webservice
WSP 1c Test	Økonomistyrrelsen	
WSP for It-og Telestyrrelsen Both and all WSC	IT- og Telestyrrelsen	
WSP for It-og Telestyrrelsen Both and approved WSC	IT- og Telestyrrelsen	✓

3

Der vises nu stamdata for webservicen og evt. privileger hvis webservicen har disse. Man vælger de ønskede privileger og trykker Send anmodning.

Ved Send anmodning bliver der sendt en mail til service providers administrator, og der startes et systembruger anmodnings flow (se 7.31).

Stamdata for webservice		
Navn	Web service udbyder	CVR-nummer
WSP for It-og Telestyrrelsen Both a	IT- og Telestyrrelsen	26769388
Kort engelsk beskrivelse af it-systemet	Version af metadata registreret i NemLog-in	Entity Id
test	1	https://saml.WSPBothApproved2.e

Administratorer for webservice udbyder		
Navn	E-mail	Telefonnummer
Sandra Bundgaard	SandraBundgaard@kfobs.dk	

Ønskede privilegier til webservice					
	Privilegium	Navn	Beskrivelse	Gælder fra	Udløber
☐	Test Sys WSP 15	https://SysWSP15.ph	test	09-03-2015 00:00:00	
☐	Test Sys WSP 16	https://SysWSP16.ph	test	09-03-2015 00:00:00	

Send kommentar til webservice administrator	
Kommentar	

Løs opgaver

[Provisioner til integrationstest](#)
[Provisioner til produktion](#)
[Skift system bruger ejer](#)
[Anmod om web service adgang](#)

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.30 Supporter systembruger

1

Ved oprettelse af en webtjeneste er det muligt at bestemme om denne skal supportere systembrugere. I drop-down menuen vælges enten "Web service med systembrugere" eller "Begge typer".

Vælges en af disse vises også en checkbox, Kun adgang for godkendte systembrugere, hvor det er muligt at angive om man kun vil give adgang til godkendte systembrugere.

Brugermanual

Integration Produktion

EntityID hentet fra metadatafilen. ?

Krypteringscertifikat hentet fra metadatafilen

Udløbsdato ?

Type af webservice

- Kun Bruger identitet baseret web service
- Web service med systembrugere
- Begge typer

☐ Kun adgang for godkendte systembrugere

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.31 Godkend eller afvis systembrugeranmodning til webtjeneste

1

Når en systembruger har ansøgt om adgang til en webtjeneste vil der blive oprettet en task under ventende opgaver til administratoren for webtjenesten. Nu kan administratoren godkende eller afvise ansøgningen som vist på billedet. Har ansøgeren også ansøgt om system privileger vil disse også blive vist.

Opgave

Anmod om adgang til web service for WSP for Økonomistyrelsen Both Access and ...

Opgavebeskrivelse Modtaget 15-05-2015

Systembrugeradministratoren for organisationen: Økonomistyrelsen CVR:10213231 anmoder om adgang til web service WSP for Økonomistyrelsen Both Access and Approved WSC

Systembrugeradministratoren har også anmodet om følgende privilegier:

- ☒ https://SysWSP7.ph
- ☒ https://SysWSP8.ph

Vælg de/det privilegie(r), du ønsker at tildele, for du trykker på godkend knappen.

Kontaktinformation for systembruger og administrator:

Systembruger EntityID: https://wsc.UserOrgOkono1.env

Systembruger administrator: Morten Mortensen

Bruger	Dato	Handling	Besked
Listen er tom			

< Tilbage Godkend Afvis

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.32 Tildel og fjern system privileger til systembrugere

1

Det er muligt for en web service administrator at tildele eller fjerne system privileger til systembrugere. Vælg først it-systemer, derefter vælger du den webservice du ønsker at arbejde med, og til sidst vælges stamdata i Løs opgaver menuen til venstre.

WSP for It-og Telestyrelsen Both and approved W...

The screenshot shows the 'WSP for It-og Telestyrelsen Both and approved W...' configuration page. The left sidebar has 'It-systemer' selected. The main area shows configuration details for a web service, including EntityID, URL, and a status table for production environments.

Integration	Produktion
EntityID hentet fra metadatafilen. https://saml.WSPBothApproved2.env	Status for tilslutning 1 2 3 4 5
Krypteringscertifikat hentet fra metadatafilen Udløbsdato 23-01-2018	Forbered produktionsmiljø
Produktion 09-03-2015 01:00:00	1 Påbegyndt 2 Produktion (ansøgt) 3 Produktion (godkendt) 4 Fuldmagt privilegie (godkendt) 5 Overfør til produktionsmiljø
Type af webservice Begge typer	Ansvarlig Teknisk administrator Teknisk administrator Administrator for it-systemudbyder NemLog-in Support
☒ Kun adgang for godkendte systembrugere	Overfør til produktionsmiljø 5 Produktion (klar)
NemLog-in komponenter	Seneste provisionering af metadata: 29-04-2015

2

Vælg fanen Systembrugere for at få en oversigt over de systembrugere som har adgang til webservice. Hvis webservices kun tillader godkendte systembrugere vil kun disse være i listen.

For webservices der kun tillader godkendte systembrugere vil det være muligt at fjerne disse ved at trykke fjern ud for brugeren.

WSP for It-og Telestyrelsen SU and approved WSC

It-systemer
 It-systemudbyder
 It-leverandør
 Brugerorganisationer
 Driftstatus
Løs opgaver
 Tilføj ny it-leverandør
 Tilføj teknisk administrator
 Rediger tekniske oplysninger om it-systemet
 Slet it-systemet
 Administration af privilegier til web service

Standarddata for it-system
 It-systemnavn
 WSP for It-og Telestyrelsen SU and approved WSC
 Kort beskrivelse af it-systemet (hvis kan slubrugernes benytte det til)
 test
 Kort engelsk beskrivelse af it-systemet
 test
 Gem standarddata

It-systemtype
 Webtjeneste
 It-systemudbyder
 IT-og Telestyrelsen
 Tildringsstatus for seneste version af metadata registreret hos NemLog-in
 Produktion (klar)
 Status for seneste version af metadata registreret hos NemLog-in
 1

Om WSP for It-og Telestyrelsen SU and approved WSC

Teknisk adm... It-leverandør Metadata... Administrat... Systembrug...

Denne liste indeholder alle godkendte brugere. Klik på linket for at fjerne en bruger. Klik på "Tildel system privilegier" for at tildel et system privilegier

Systembrugere			
Navn	CVR-nummer	EntityID	
WSP for Itog Serv Prov	26769388	https://wsc.ServProvItog.env	Fjern

3

Ved at klikke på Administration af privilegier til web service eller direkte på brugeren i listen er det muligt at tildele en systembruger privilegier til web servicen.

Linket Administration af privilegier til web service vil kun være tilgængeligt hvis web servicen har system privilegier.

Hvis webservicen kun tillader godkendte systembrugere vil kun det kun være muligt at tildele disse brugere privilegier.

Løs opgaver

[Tilføj ny it-leverandør](#)

[Tilføj teknisk administrator](#)

[Rediger tekniske oplysninger om it-systemet](#)

[Slet it-systemet](#)

[Administration af privilegier til web service](#)

4

Når der er valgt hvilken bruger der skal tildeles privilegier kan man slette privilegier ved at trykke på Fjerne ud for det pågældende privilegier

Ønsker man at tildele systemprivilegier vælges Tildel privilegier i menuen til venstre.

Hjem > It-systemer > WSP for It-og Telestyrelsen SU and approved WSC > Detaljer om systembruger

Systembruger Detaljer

It-systemer
 It-systemudbyder
 It-leverandør
 Brugerorganisationer
 Driftstatus
Løs opgaver
 Tildel privilegier

Detaljer om systembruger
 EntityID
 https://wsc.ServProvItog.env
 Dato godkendt
 12-03-2015 02:05:20
 Beskrivelse
 WSC for Itog Serv Prov
 CVR
 26769388
 Navn
 WSC for Itog Serv Prov

Tildelte privilegier

Navn	Beskrivelse	It-systemudbyder	
https://SysWSP11.ph	Test Sys WSP 11		Fjerne
https://SysWSP12.ph	Test Sys WSP 12		Fjerne

5

Herefter kan man vælge privilegierne man ønsker at tildele ved at klikke dem af og afslutte med at klikke på Tildel Privilegie knappen.

Hjem » It-systemer » WSP for It-og Telestyrelsen SU and approved WSC » Systembrugere »

Tildel privilegie

It-systemer

It-systemudbyder

It-leverandør

Brugerorganisationer

Driftstatus

	Privilegium	Navn	Beskrivelse	Gælder fra	Udløber
☒	Test Sys WSP 11	https://SysWSP11.ph	test	09-03-2015 00:00:00	
☐	Test Sys WSP 12	https://SysWSP12.ph	test	09-03-2015 00:00:00	

< Tilbage

Tildel privilegie

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

7.33 Tilføj test systembruger

1

Vælg et it-system. Åbn detaljer for it-systemet ved at klikke på systemnavnet.

2

Vælg fanen Integration og tryk på Tilføj test systembruger i Løs opgaver menuen til venstre.

3

Tryk Vælg test systembruger

Oprettelse af testbruger

CVR-nummer*

EntityId for systembruger*

Vælg test systembruger

4

Vælg den ønskede bruger og tryk OK.

Test systembruger

 Søg i oversigten:

	Navn	CVR-nummer	EntityId for systembruger
☐	https://wsc.expiredOkonoFoces.env	10213231	https://wsc.expiredOkonoFoces.env
☐	https://wsc.expiredOkonoVoces.env	10213231	https://wsc.expiredOkonoVoces.env
☐	https://wsc.revokedOkonoFoces.env	10213231	https://wsc.revokedOkonoFoces.env
☐	https://wsc.revokedOkonoVoces.env	10213231	https://wsc.revokedOkonoVoces.env
☐	https://wsc.ServProvItog.env	26769388	https://wsc.ServProvItog.env
☐	https://wsc.ServProvOkono1.env	10213231	https://wsc.ServProvOkono1.env
☐	https://wsc.UserOrgItog.env	26769388	https://wsc.UserOrgItog.env
☐	https://wsc.UserOrgOkono1.env	10213231	https://wsc.UserOrgOkono1.env

5

Tilføj privilegier til testbrugeren ved at vælge privilegierne og tryk på knappen 'Tilføj privilegie til testbruger'

Tilføj privilegie til testbruger

☐ Vælg alle	Navn	Privilegium
☒	Citizen priv auto 1	https://delegation.ph
☐	System priv auto 1	https://sysprivpop1.ph

6

Afslut ved at trykke på Opret Testbruger

Funktionen er tilgængelig for rollerne:

- Teknisk administrator

8 Drift Status

For at se drift status menu i CSS, skal Nemlogin Administrator være logget ind i administrationsportalen.

1

Klik på 'Drift Status' fanebladet for at se hvordan kan man "editere drift beskeder og" tilføjer eller redigere template".

The screenshot shows the 'NemLog-in/Administration' web interface. The top navigation bar includes 'Hjem', 'Ventende opgaver', 'Supportadministration', and 'Hjælp'. The user is logged in as 'Morten Mortensen' with a 'Log ud' button. The left sidebar lists categories: 'It-systemer', 'It-systemudbydere', 'It-leverandør', 'Brugerorganisationer', and 'Driftstatus' (highlighted in orange). The main content area is titled 'Draft Status' and contains two tabs: 'Editor drift ...' and 'Tilføj eller redig template'. The 'Editor drift ...' tab is active, showing a form with the following fields: 'NemLogin Nøglekort' (dropdown), 'NemLogin Nøglekort' (text), 'Normal drift status' (dropdown), 'Planlagt status' (dropdown), 'Start dag' (calendar icon), 'Slut dag' (calendar icon), 'Nedbrud' (dropdown), and a 'Gem' button.

2

Gå til fanebladet "tilføj eller redig template" og klik på "Tilføj ny template" og give Intern Beskrivelse, Status DK, Status EN og tryk på Gem.

Funktionen er tilgængelig for rollerne:

- NemLog-in administrator