

OS2faktor

Opsætning af MitID Erhverv

1 Indledning

Denne vejledning er udarbejdet med input fra MitID Erhverv piloterne, og materiale fra både Næstved og Viborg Kommune er indarbejdet hvor relevant. Stor tak til piloternes arbejde, og deres input til denne guide.

Alle kommuner skal igennem tilslutningen til MitID Erhverv, da denne portal fremover skal anvendes til hhv

- Udstedelse og administration af certifikater (de nye OCES 3 certifikater der erstatter de gamle funktions- og virksomhedscertifikater)
- Oprettelse og administration af medarbejdere og deres rettigheder

Da MitID Erhverv portalen først er tilgængelig EFTER man har gennemført en import af eksisterende brugere fra det gamle Virk brugeradministration (også kaldet NemLog-in brugeradministration eller NemID Erhverv brugeradministration), så er man nødt til at gennemføre denne bruger-import, for at komme til at udstede OCES 3 certifikater.

Det betyder at hvis man først har planlagt NSIS revision ude i fremtiden, og ikke er klar til at tage MitID Erhverv i brug for brugere, så skal man alligevel gennemføre importen af brugere nu, da man ellers ikke kan tilgå certifikat-administrationen.

1.1 Opmærksomhedspunkter vedrørende brugerimporten

Det er uheldigt at flere årsager, at man er nødt til at udføre importen af brugere før man er klar til at tage brugeradministrations-delen af MitID Erhverv i brug, men der er desværre ikke så meget at gøre ved det.

Man skal være opmærksom på følgende når man foretager importen af brugere

1. Man kan kun udføre importen én gang. Det betyder at alle brugere man opretter i det gamle brugeradministrations-system EFTER importen, også skal oprettes i MitID Erhverv, da disse ikke importeres automatisk.
2. Der vil blive sendt en email fra MitID Erhverv til alle importerede brugere. Denne sendes 30 dage efter importen (med mindre man aktiverer brugerne, I så fald sendes mailen med det samme). Denne mail kan ikke undgås, så man kan med fordel informere medarbejderne om at den kommer. Da I er nødt til at aktivere jeres administratorer, kan I se indholdet af denne email når den ankommer til jeres administratorer efter aktiveringen.

2 Overblik over aktiviteter

Processen er langt hen af vejen den samme for alle kommuner, og bortset fra mindre ændringer i rækkefølgen (afhængig af hvornår man revideres), så skal alle gennem følgende skridt

1. Kommunen skal tilslutte sit MitID Erhverv
2. Under tilslutningen skal kommunen vælge hvilke administratorer fra det gamle brugeradministration der skal importeres, samt hvilke af deres administrator-rettigheder der skal overføres til MitID Erhvervs brugeradministration
3. Endeligt skal man vælge at importere alle eksisterende brugere. Man kan også vælge at springe importen over, men hvis man gør det, så skal man manuelt oprette samtlige brugere i MitID Erhverv, og et anbefales ikke. Importerede brugere får også deres

rettigheder overført, så det er en betydelig nemmere måde at håndtere det på (med respekt for de opmærksomhedspunkter der er nævnt i afsnit 1.1)

Herefter kan ens administratorer logge ind i MitID Erhverv, og man kan administrere certifikater. Bemærk at administratorerne er nødt til at foretage login med deres private MitID indtil de efterfølgende trin er gennemført. De næste trin forudsætter at man har gennemført revisionen og er blevet optaget på Digitaliseringsstyrelsens positivliste

4. Anmod Digitaliseringsstyrelsen om adgang til at oprette lokal IdP og anvende lokal IdM
5. Opret et lokal IdM certifikat til Digital Identity – dette gør det muligt for OS2faktor løsningen at udføre opdatering og aktivering af alle importerede brugere
6. Opret en lokal IdP
7. Sammen med Digital Identity laves en CSV/Excel fil, der indeholder alle importerede brugere i MitID Erhverv, med deres RID numre, matchet op mod den AD konto i kommunes infrastruktur som skal bruges til login fremtidig
8. Digital Identity udfører en opdatering af alle importerede brugere, hvor manglende oplysninger (fødselsdato, navn, osv) udfyldes korrekt, og den valgte AD konto tilknyttes som et lokalt loginmiddel – og alle brugerkonti aktiveres.

Herefter kan brugerne foretage login til de forskellige tjenester koblet på NemLog-in/MitID Erhverv vha OS2faktor IdP'en, og dermed ved at bruge deres AD brugernavn/kodeord samt deres OS2faktor MFA klient til step-up.

Hvis kommunen anvender OS2rollekatalog er der yderligere trin der kan opsættes, der gør det muligt for kommunen at trække alt rettighedsstyring ud af MitID Erhverv portalen, og udføre denne via OS2rollekatalog i stedet. Denne opsætning består af følgende trin

9. Digital Identity trækker alle tilgængelige rettigheder ud af MitID Erhverv og indlæser dem som rettigheder under et it-system med navnet "NemLog-in" inde i OS2rollekatalog
10. Kommunen kan nu oprette Jobfunktionsroller og tildele disse til brugere via OS2rollekatalog, og de vil have samme effekt som direkte tildelte rettigheder inde i MitID Erhverv portalen

Der er pt en afklaring igang i OS2rollekatalog koordinationsgruppen om håndteringen af eksisterende rettigheder i MitID Erhverv portalen – det forventes at løsningen ender med at alle disse migreres ind i OS2rollekatalog, så man har ét samlet overblik over rettigheder i OS2rollekatalog.

3 Vejledning

Nedenstående vejledning er en mere detaljeret gennemgang af de enkelte punkter fra ovenstående liste. Hver aktivitet har sin egen beskrivelse, med tilhørende screenshots hvor relevant

3.1 Tilslutning til MitID Erhverv

I har formodentligt allerede modtaget kommunikation fra Digitaliseringsstyrelsen om hvordan I gennemfører selve aktiveringen. Processen startes inde fra

<https://tilslut.nemlog-in.dk/>

og processen skal opstartes af en ledelsesrepræsentant i kommunen. I forbindelse med denne proces kan ledelsesrepræsentanten udpege en anmelder, som håndterer den praktiske tilslutning efter den initielle accept er foretaget af ledelsesrepræsentanten.

Bemærk at ledelsesrepræsentanten under første tilslutning skal uploade dokumentation for at de er ledelsesrepræsentant, og at Digitaliseringsstyrelsen har en manuel verifikationsprocedure der kan tage op til 10 arbejdsdage.



Dokumentér at du er ledelsesrepræsentant

Nedenfor skal du uploade dokumentation, der viser, at du er ledelsesrepræsentant for organisationen.

> [Læs mere om krav til dokumentation](#)

Dokumentation for tilknytning til organisationen som ledelsesrepræsentant

> [Vigtigt: Læs om krav til dokumentation](#)

[HjemmesideMedl.edelse.pdf](#)  Fjern dokumentet

[Tilbage](#)

Du kan finde hjælp her:
[Veiledning til tilslutning](#)

Som dokumentation kan man bruge referat fra kommunalbestyrelsesmøde, screenshot eller link til kommunens officielle hjemmeside hvor ledelsesrepræsentanten er nævnt, eller anden dokumentation for at personen er ledelsesrepræsentant.

Det anbefales at ledelsesrepræsentanten udpeger en organisationsadministrator (fx en af de eksisterende administratorer i det gamle brugeradministration) under tilslutningen, da man ellers kan risikere at blive låst ude af systemet.

3.2 Tilslutning / opsætning af MitID Erhverv

Den udpegede anmoder / organisationsadministrator vil modtage en aktiveringsemail med et link til at gennemføre selve opsætningen. Dette link er gyldigt i 60 dage, og aktiveringen skal afsluttes indenfor denne tidsfrist.

Når man anvender linket, og gennemfører login (med privat MitID), så mødes man af en aktiverings "wizard", der guider en gennem aktiveringsforløbet.

Skærbilledet man ser skulle gerne ligne nedenstående

Opgaver du skal løse Afbryd

Her kan du se de opgaver, du skal igennem for at lave opsætningen.

Når du har udført en opgave, bliver det markeret i overblikket. Så kan du vende tilbage til den opgave, du var nået til, hvis du ikke gennemfører opsætningen på én gang.

Opgaver	Status
Importér administratorer og brugere	● Ikke udført
Fakturering	● Ikke udført
Organisationens identifikationsmidler	● Ikke udført
Vælg dine egne identifikationsmidler	● Ikke udført

[Veiledning til opsætning](#)
Næste

Første trin er ret ligetil, da man præsenteres for en liste af eksisterende administratorer og deres rettigheder. Her kan man vælge hvilke der skal overføres. Med mindre man har administratorer som ikke længere er ansat, eller ikke skal være administratorer mere, så vil man formodentligt blot importere alle administratorere med de rettigheder de har i dag.

Når man kommer til de almindelige brugere, så skal de ligeledes importeres. Man kan vælge at undlade importen af eksisterende brugere, men så skal man manuelt oprette dem og tildele dem rettigheder, så det anbefales ikke.

Fakturerings-trinnet er formodentligt bare at acceptere de allerede opsatte oplysninger, og der skal ikke gøres noget yderligere her.

Til trinnet om organisationens identifikationsmidler, spørges man om hvorvidt brugerne skal have lov til at bruge deres private MitID til login. Det handler om det dobbelte frivillighedsprincip, og giver alene jeres medarbejdere MULIGHED for at bruge privat MitID til login, men påtvinger ikke nogen brugere anvendelsen af privat MitID.

Skal brugerne kunne anvende deres private MitID? [Afbryd](#)

Alle brugere skal have et MitID identifikationsmiddel fx en MitID app for at kunne logge ind eller skrive under digitalt på vegne af en organisation.

Du kan tilbyde, at brugerne kan anvende deres private MitID på vegne af jeres organisation. Så behøver brugerne kun det ene MitID.

> [Læs mere om brug af privat MitID](#)

Ja, organisationen accepterer brug af privat MitID

Nej, organisationen accepterer IKKE brug af privat MitID

[Vejledning til opsætning](#) [Tilbage](#) [Næste](#)

Endeligt skal du, som administrator, angive hvordan du vil logge ind fremover. Der er reelt ikke så mange muligheder end at vælge privat MitID, og det er nødvendigt i opsætningsperioden, da den lokale IdP (OS2faktor) ikke er tilsluttet endnu på dette tidspunkt.

Herefter er opsætningen afsluttet, og man kan foretage login til MitID Erhverv portalen her

<https://erhvervsadministration.nemlog-in.dk/>

Efter login vil man bemærke at man har følgende menupunkter i venstre-menuen



Brugere vil alene indeholde ganske få brugere, da kun de brugere har været involveret i tilslutningen er blevet aktiveret. Alle importerede brugere ligger nede under "Importerede brugere" og er ikke aktiverede endnu.

Her kan man vælge at gå ned og finde de administratorer, som man gerne vil have aktiveret her og nu, og så aktivere disse. Bemærk at der kan mangle oplysninger på disse brugere (fx fødselsdato), som skal udfyldes før de kan aktiveres.

OBS! Undlad at aktivere andre brugere end administratorerne. OS2faktor kan udføre denne aktivering for jer når I er blevet revideret og optaget på Digitaliseringsstyrelsens positivliste.

3.3 Anmode om at gøre brug af lokal Identity Provider

Forudsætningen for at gå igang med dette trin, er at man er optaget på Digitaliseringsstyrelsens positivliste, som kan findes her

<https://digst.dk/it-loesninger/standarder/nsis/>

Til selve tilslutningen har Digitaliseringsstyrelsen publiceret en vejledning, som kan hentes her

<https://www.mitid-erhverv.dk/info/losning/vilkar/>

det er Bilag 7 på siden. Den er nogenlunde overskuelig, og de ter model 1 (lokal IdP hos Brugerorganisationen) som anvendes.

Det bør dermed ikke være nødvendigt at udfylde Bilag A i Bilag 7, da denne vedrører scenariet hvor en 3.part har det fulde ansvar for NSIS revisionen – dvs at man alene skal skrive til

mitiderhverv@digst.dk

3.4 Opsætning af OS2faktor

Når anmodningen er godkendt hos Digitaliseringsstyrelsen, bookes et møde med Digital Identity (kontakt@digital-identity.dk), hvor vi i fællesskab sætter resten af tilslutningen op inde i MitID Erhverv. Her skal vi gennem følgende trin

- Bestille et certifikat, der giver adgang til IdM API'et
- Opsætte en Lokal Identity Provider
- Tilpasse opsætningen, så lokale loginmidler er mulige
- Opsætte lokale loginmidler på de administratorer som allerede er aktiveret

Disse ting gøres alle i fællesskab i MitID Erhverv portalen.

3.5 Aktivering af importerede brugere

Endeligt skal der udføres en aktivering af alle de brugere som findes under "importerede brugere". Dette håndteres på følgende måde

- Til hver importeret bruger skal der knyttes et AD brugernavn
- Hver bruger skal have opdateret evt manglende informationer (navn, fødselsdato, osv)
- Endeligt skal brugeren aktiveres (brugeren rykkes op under brugere, og MitID Erhverv sender dem en velkomst email hvis de ikke allerede har modtaget den)

Alt dette håndteres automatisk af OS2faktor, men det forudsætter at OS2faktor er udstyret med en liste af RID numre og AD brugernavne, så den ved præcist hvilket RID nummer som hører til hvilken AD konto. En sådan liste kan evt trækkes fra kommunens Signaturcentral, eller fra medarbejdersignatur-portalen. OS2faktor behøves ikke nødvendigvis få AD brugernavnet, en email adresse eller cpr nummer kan også være nok.

Digital Identity sammenholder listen med de indlæste data i OS2faktor, og danner en liste over brugere som der måtte give problemer, dette kan bl.a. være

- Ansatte som har flere RID numre (men kun ét AD brugernavn) – man kan desværre ikke knytte det samme AD brugernavn til flere RID numre
- Brugerkonti som findes i MitID Erhverv, men som ikke har en AD konto i kommunens AD (fx eksterne eller personer som ikke længere er ansatte)

Kommunen og Digital Identity afgør sammen hvad der skal ske med disse brugere, hvorefter opdateringen udføres, og alle brugerkonti aktiveres.

Evt resterende brugere under "importerede brugere" kan kommunen vælge at slette, eller tildele et MitID loginmiddel (fx en mulighed for eksterne som ikke findes i kommunens AD).

Herefter håndterer OS2faktor automatisk brugeroprettelse og brugernedlæggelse i MitID Erhverv, på baggrund af styring fra kommunens AD (eller OS2rollekatalog hvis man gør brug af dette).

3.6 Opsætning af OS2rollekatalog

På bagkant af ovenstående opsætning, kan Digital Identity også opsætte OS2rollekatalog som styrende for rettigheder i MitID Erhverv. Dette er en ren teknisk opsætning, som gør det muligt for kommunen at se og tildele rettigheder i MitID Erhverv, via OS2rollekatalogs brugergrænsefladen.

Tag fat i kontakt@digital-identity.dk for at få dette sat op.

4 Loginoplevelsen

Når OS2faktor er opsat som Identity Provider mod NemLog-in, så vil brugerne opleve følgende loginflow når de skal tilgå tjenester tilsluttet NemLog-in. Eksemplet er illustreret via et login til skat.dk

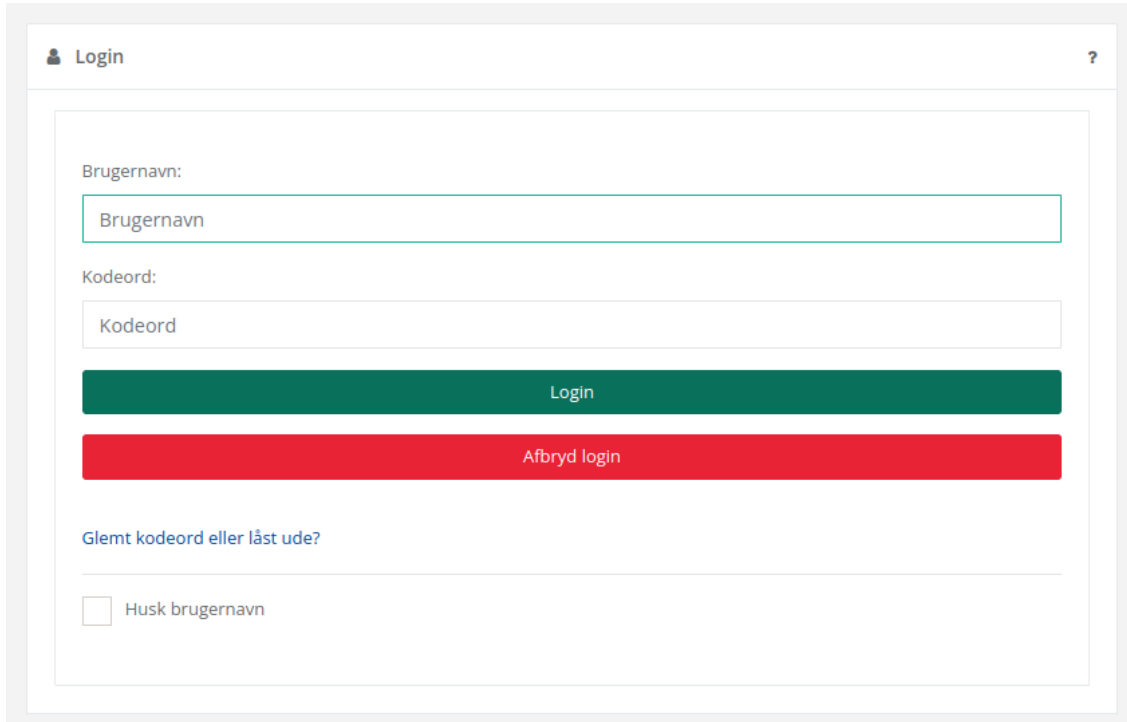
1 – brugeren tilgår tjenesten og klikker på "Log på"



2 – brugeren sendes til NemLog-in, hvor der vælges "Lokal IdP" samt kommune



3 – brugeren logger på OS2faktor (evt via single sign-in)



Login

Brugernavn:
Brugernavn

Kodeord:
Kodeord

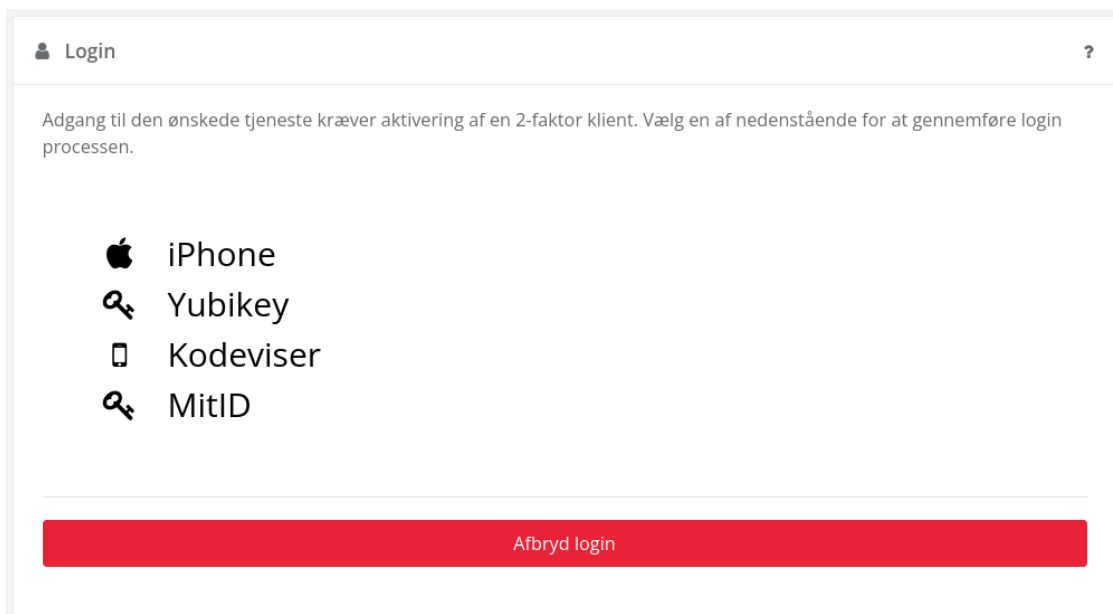
Login

Afbryd login

[Glemte kodeord eller låst ude?](#)





Husk brugernavn

4 – brugeren anvender sin 2-faktor klient



Login

Adgang til den ønskede tjeneste kræver aktivering af en 2-faktor klient. Vælg en af nedenstående for at gennemføre login processen.

-  iPhone
-  Yubikey
-  Kodeviser
-  MitID

Afbryd login

5 – brugeren er nu logget ind i den valgte tjeneste