

OS2faktor

Opsætning i MitID Erhverv

Version: 1.0.0

Date: 13.06.2023

Author: BSG

1 Indledning

I forbindelse med ibrugtagning af MitID Erhverv, skal der opsættes en integration fra OS2faktor til MitID Erhverv. Dette dokument beskriver den opsætning der er nødvendig

2 Indhente oplysninger

I forbindelse med opsætningen er der en række oplysninger som er nødvendige. Disse er

- Mapping mellem AD brugernavn og RID på eksisterende brugere
- Default e-mail adresse til brugere uden email
- Metadata fil fra OS2faktor installationen

Den sidste er blot en bagstopper til de brugere som af den ene eller anden årsag ikke har en email adresse. Da email adressen er et krævet felt ved brugeroprettelse i MitID Erhverv, er der brug for en default værdi som kan indtastes på disse brugere.

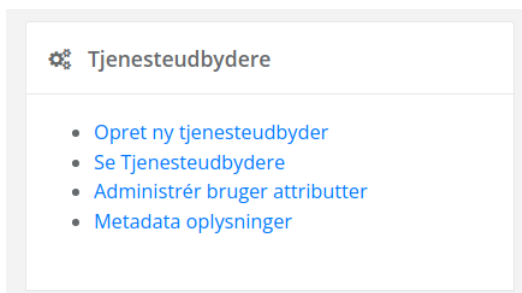
Vælg evt en systempostkasse i kommunen, som modtager de informationsmails som Digitaliseringsstyrelsen evt vil sende til den angive email adresse. Der er ikke nogen kritisk funktion bundet op på email adressen, så brugerne behøves ikke modtage mailen for at funktionaliteten vil fungere.

Mht mappingen mellem AD brugernavne og RID numre, så skal denne information bruges til migreringen af eksisterende brugere. Man kan trække en sådan liste inde fra Signaturcentralen, hvor man med fordel kan angive at man kun vil have aktive brugere med ud i excel rapporten.

Både email og AD/RID rapporten skal sendes til Digital Identity, evt ved upload på

<https://kundenet.digital-identity.dk/>

Metadata filen fra OS2faktor kan hentes inde fra selvbetjeningen. Log ind i selvbetjeningen og tilgå menupunktet "Metadata oplysninger" under administration



Her er der et link direkte til SAML 2.0 metadata filen, fx som vist her (det faktiske link er kundespecifikt)

SAML 2.0

Tjenesteudbyderen kan hente alle SAML metadata via net automatisk opdage når certifikater opdateres i OS2faktor

<https://demo-idp.os2faktor.dk/sso/saml/metadata>

Ved klik på linket vises en side med metadata indholdet, fx

`<this XML file does not appear to have any style information associated with it. The document t`

```

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ID="_077
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumerat
    <md:KeyDescriptor use="signing">
      <md:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIGHTCCBQWgAwIBAgIEXimFozANBqkqhkiG9w0BAQsFADBA
MTRaFw0yNDExMTUwNzEzMDRaMIGQMqswCQYDVQGEwJESzEtMCSGA1UECgwkRELSVRB1
ODI4MC4GA1UEAwWnUG9jSW50ZWdyYXRvcjIwMjEgKz1bmt0aW9uc2N1cnRpZmRlRlRyYQ
p5K/0KI/iWtHyoh3wAcAzqEcqb09/NHYiuUVsmqY8gJcW/U6+yHJtj0zEXuneieIaAsc
AQABo4ICzDCCAsGdgYDVR0PAQH/BAQDAg04MIGJBggrBgEFBQCBAQR9MHswNQYIKwYB
dHRwOi8vZi5haWUuawWnMDQudHJ1c3QyNDA4LmNvbS59vY2VzLWZc3VpbmcwN1jYS5j
LnRydXN0MjQwOC5jb20vcWVwb3NpdG9yeTCB7gYIKwYBBQUHAgIwgeEwEBYJVFJVVU1Qy
UFMgb2cgT0NFUyB0UCwZGVyIGthbiBoZW50ZXMGZnJhIHd3dy50cnVzdDI0MDguY29t
c2V0IGFuc3ZhciBpZnQuIHByb2ZlcnNpb251bGx1IHhcnRlcj4wZGZcGA1UdHwSBjzCBj
BgNVBAYTAKRMRiEAYDVOQKDALUULVTVDI0MDgxHTAbBgNVBAMFFRSVNUMjQwOCBPC
A1UdDgQWBBCmgKumbqFHxaHW05FXeFY9TKEbjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEB
Cm74KsZWUcc70gWFr2zucPaPoELQwf0CbWHIss0YHDni2gKLVJdhL2IyVxoETL7miQX:
9apopL0ggJJ4o9Ixxf1tfzz0a09B4T7hki6Q60VhYNF11XV5CC4o0oyA/kcTBHScDAo:
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <md:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIGHTCCBQWgAwIBAgIEXimFozANBqkqhkiG9w0BAQsFADBA
MTRaFw0yNDExMTUwNzEzMDRaMIGQMqswCQYDVQGEwJESzEtMCSGA1UECgwkRELSVRB1
ODI4MC4GA1UEAwWnUG9jSW50ZWdyYXRvcjIwMjEgKz1bmt0aW9uc2N1cnRpZmRlRlRyYQ
p5K/0KI/iWtHyoh3wAcAzqEcqb09/NHYiuUVsmqY8gJcW/U6+yHJtj0zEXuneieIaAsc
AQABo4ICzDCCAsGdgYDVR0PAQH/BAQDAg04MIGJBggrBgEFBQCBAQR9MHswNQYIKwYB
dHRwOi8vZi5haWUuawWnMDQudHJ1c3QyNDA4LmNvbS59vY2VzLWZc3VpbmcwN1jYS5j
LnRydXN0MjQwOC5jb20vcWVwb3NpdG9yeTCB7gYIKwYBBQUHAgIwgeEwEBYJVFJVVU1Qy
UFMgb2cgT0NFUyB0UCwZGVyIGthbiBoZW50ZXMGZnJhIHd3dy50cnVzdDI0MDguY29t
c2V0IGFuc3ZhciBpZnQuIHByb2ZlcnNpb251bGx1IHhcnRlcj4wZGZcGA1UdHwSBjzCBj
BgNVBAYTAKRMRiEAYDVOQKDALUULVTVDI0MDgxHTAbBgNVBAMFFRSVNUMjQwOCBPC
A1UdDgQWBBCmgKumbqFHxaHW05FXeFY9TKEbjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEB
Cm74KsZWUcc70gWFr2zucPaPoELQwf0CbWHIss0YHDni2gKLVJdhL2IyVxoETL7miQX:
9apopL0ggJJ4o9Ixxf1tfzz0a09B4T7hki6Q60VhYNF11XV5CC4o0oyA/kcTBHScDAo:
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
    </md:EntityDescriptor>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

Og da man ikke på nuværende tidspunkt kan linke til metadata inde fra MitID Erhverv (send endeligt et ændringsønske til Digitaliseringsstyrelsen på dette, så opdatering af metadata kan ske automatisk i fremtiden), så skal man højreklikke og vælge at downloade filen til sit skrivebord (gem den fx som metadata.xml).

3 Opsætte loginmidler i MitID Erhverv

Inde i MitID Erhverv vælges "Indstillinger" i højremenuen, og så scrolles ned til "Identifikationsmidler"

Identifikationsmidler

Alle brugere skal have et 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. Du skal også

Nederst i denne sektion kan man tilvælge at lokale loginmidler må anvendes. Sæt flueben i dette felt.

Herefter er det muligt at tildele lokale loginmidler til brugerne (dette håndterer OS2faktor automatisk for jer)

4 Opsætte Lokal IdP i MitID Erhverv

Længere nede i listen over indstillinger ligger "Lokal IdP". Her vælger man at tilslutte en ny Lokal IdP, hvorefter man skal gennem 4 sideres opsætning.

På første side angiver man et navn (det er det navn jeres brugere ser, så vælg kommunens navn, fx "Næstved Kommune"), samt sikringsniveau (Betydelig) og type af IdP (OIOSAML 3.0.3).

På næste side skal man uploade metadata filen – den der blev hentet fra OS2faktor.

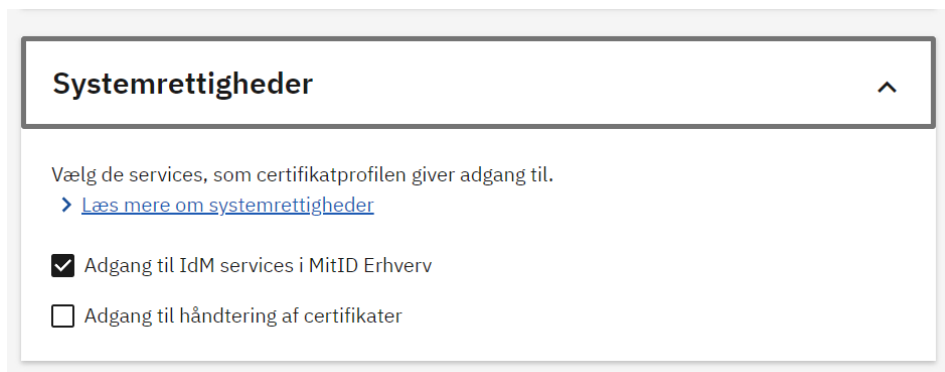
På tredje side skal man blot sige ok/næste, da kommunens CVR nummer allerede er tilvalgt.

På sidste side skal man blot acceptere opsætningen.

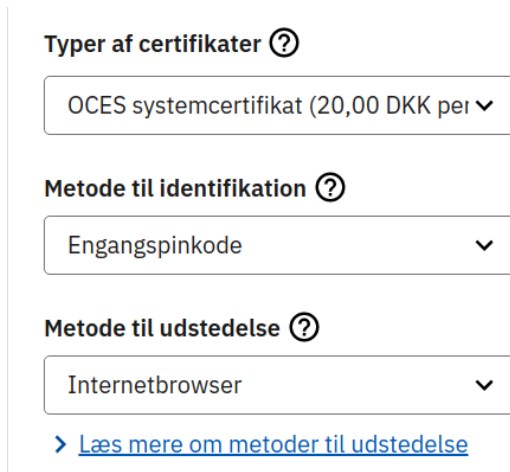
Nu er det muligt at vælge egen kommune under Lokal IdP når man logger ind med NemLog-in.

5 Bestille certifikat til MitID Erhverv IdM API

For at OS2faktor kan integrere med MitID Erhverv, skal der være adgang til MitID IdM API'et. Dette håndteres vha et certifikat. Bestil et nyt systemcertifikat, og på fane 2, hvor man tildeler rettigheder til certifikatet, sættes hak i "Adgang til IdM services i MitID Erhverv"



Der vælges systemcertifikat som type, og pinkode som identifikation og internetbrowser som metode.



Der vises nu en pinkode på skærmen – det er vigtigt at denne noteres, og enten sendes til Digital Identity via mail/sms, eller uploades i en TXT fil på kundenettet

<https://kundenet.digital-identity.dk/>

Herefter sender MitID Erhverv en aktiveringsmail – denne forwardes til kontakt@digital-identity.dk

Digital Identity står for udstedelsen af certifikatet, så det placeres sikkert i driftsmiljøet for OS2faktor.

6 Hvad er processen herefter

Digital Identity udfører nu følgende opgaver

- Filen med mapningen mellem AD konti og RID numre læses ind i OS2faktor
- IdM API'et på MitID Erhverv bruges til at udlæse alle brugere som ligger inder "Importerede brugere", og der laves et match på RID nummer mellem data i MitID Erhverv og brugerkonti i OS2faktor
- OS2faktor udfører nu en aktivering af alle de importerede brugere (hvor der er match på RID), hvilket resulterer i at Digitaliseringsstyrelsen sender en informationsmail til brugeren om at de skal aktivere deres MitID Erhverv. Denne mail er helt forkert, da brugerne IKKE skal aktivere deres MitID Erhverv. Mailen sendes fra noreply@mitid-erhverv.dk, så hvis den kan blokeres kan det være en fordel – ellers bør brugerne informeres på forkant om at de modtager en sådan mail, så de ved de skal se bort fra den

Fra: MitID Erhverv <noreply@mitid-erhverv.dk>
Sendt: 9. juni 2023 08:19
Til: xxxxxxxxxxxxxxxxxxxxxxxx <xxx@kommune.dk>
Emne: Aktivér din brugerprofil



Til xxxxxx

Din brugeradministrator har oprettet en brugerprofil til dig i MitID Erhverv. I fremtiden skal du bruge MitID Erhverv i stedet for din NemID medarbejdersignatur, når du skal foretage handlinger digitalt på vegne af organisationen.

Din brugerprofil bliver aktiveret næste gang, du logger ind på en offentlig tjeneste på vegne af din organisation.

Hvis du ønsker at se din brugerprofil i MitID Erhverv, skal du klikke på linket og logge ind med dit private MitID.

Se din brugerprofil her:

- Der vil være en mindre mængde brugere tilbage under importerede brugere – det er typisk brugere som ikke længere er ansat, men man kan med fordel tage et kig på dem, og så evt slette dem der ikke skal oprettes. Evt resterende brugere skal der tages hånd om – kontakt Digital Identity vedrørende dette.

Herefter er det vigtigt at man styrer hvem der skal oprettes i MitID Erhverv via den valgte kanal. Hvis man gør brug af OS2rollekatalog til formålet, så skal man fremover tildele/fjerne rettigheden til MitID Erhverv herinde, og så vil brugerne blive oprettet/nedlagt i MitID Erhverv automatisk.

Hvis man anvender AD som styring til MitID Erhverv, så skal man sikre at alle brugere der skal være i MitID Erhverv er medlem af den valgte AD sikkerhedsgruppe. Vær opmærksom på at hvis man fjerner en bruger fra AD gruppen, så spærres dere konto i MitID Erhverv.