DIGITALISERINGSSTYRELSEN

Webinar:
Sådan kan I anvende MitID Erhverv

2. november 2022, kl. 09.30-11.00

Christian Schmidt-Madsen

It-arkitekt

Digitaliseringsstyrelsen

Tage Vestergård Madsen

It-arkitekt

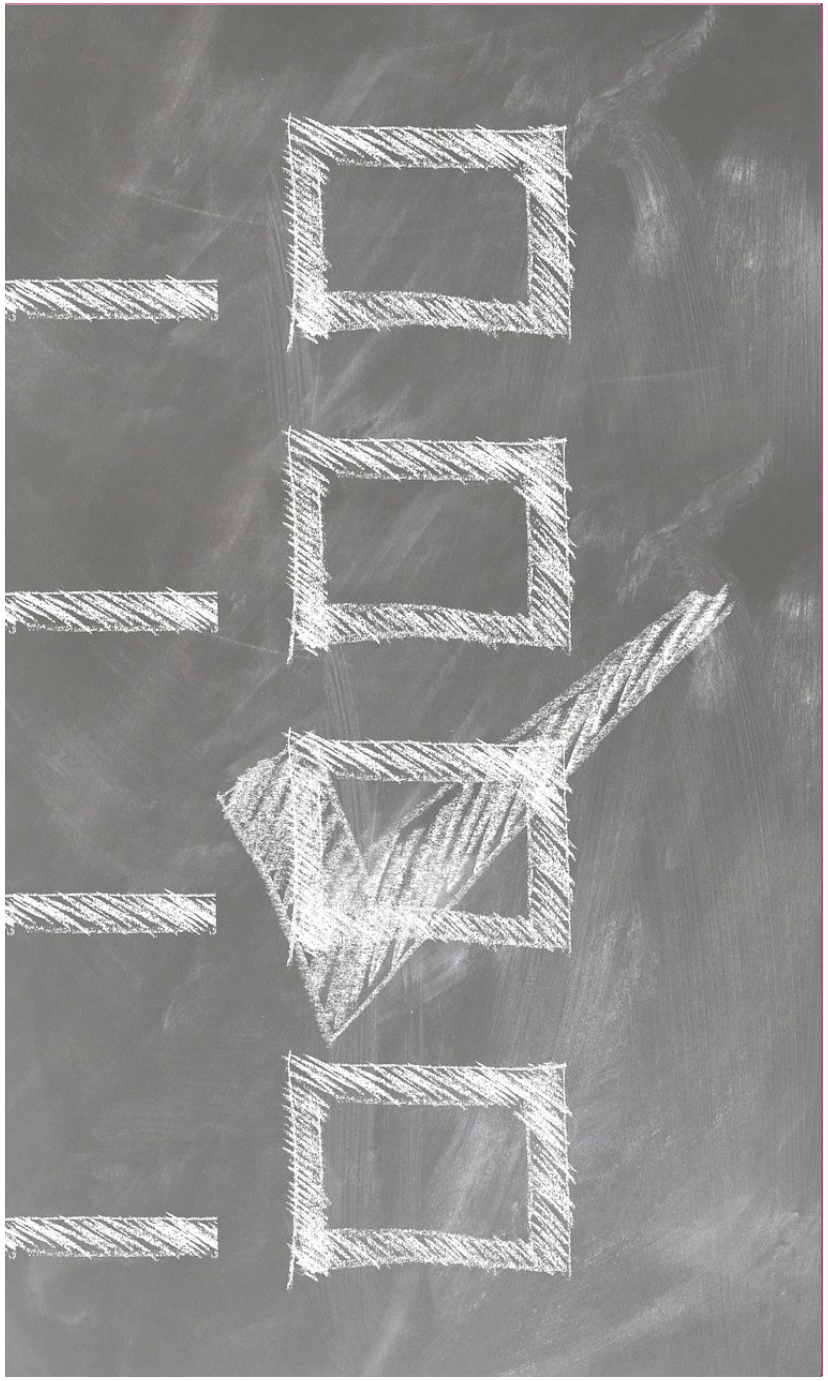
Nets

Thomas Mostrup Nymand

Løsningsarkitekt

Nets

DIGITALISERINGSSTYRELSEN



Dagsorden

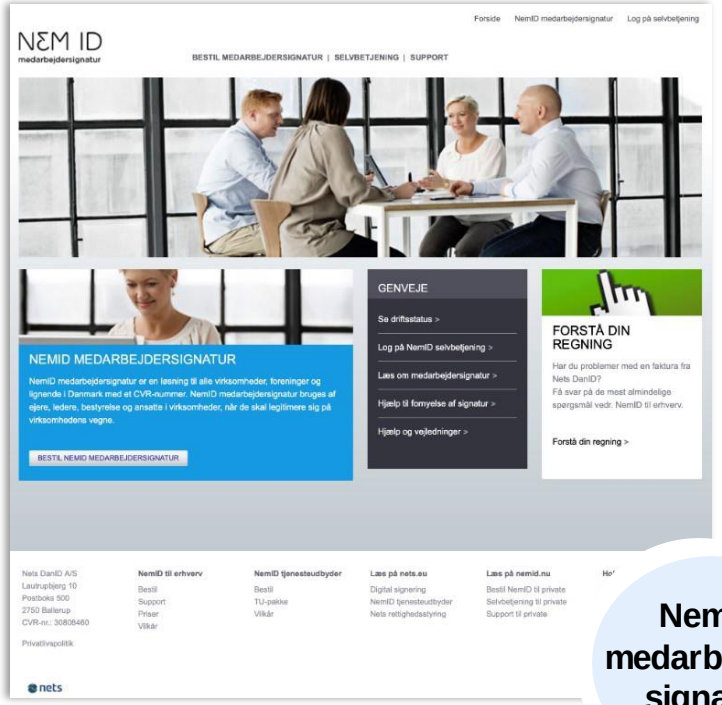
- **Velkommen + status på MitID Erhverv**
- **Del 1:**
  - **Tre modeller for anvendelse af MitID Erhverv**
  - **Sådan gør I klar til MitID Erhverv**
  - **Spørgsmål**
- **Del 2:**
  - **Masseadministration af importerede brugere**
  - **IdM-integration**
  - **Lokal IdP**
  - **Opsamling**
  - **Spørgsmål**

DIGITALISERINGSSTYRELSEN

Intro og status på MitID Erhverv

MitID Erhverv samler to systemer i ét
- erstatter NemID Erhverv og Brugeradministrationen

Administrator opretter og tildeler NemID Erhverv på medarbejdersignatur.dk…

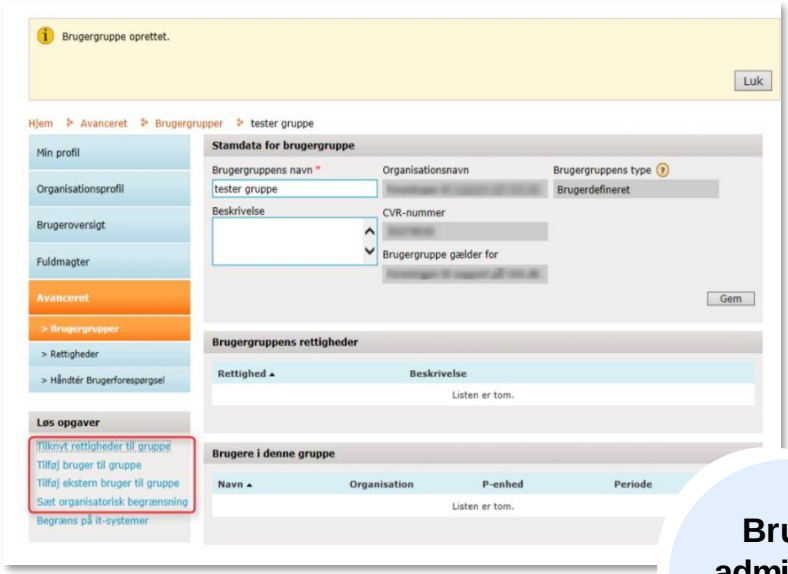


Nøglekort eller nøglefil.

Ingen mulighed for NemID nøgleapp

NemID medarbejder-signatur

…og tildeler rettigheder og fuldmagter på Brugeradministrationen (kan tilgås via Virk)



Bruger-administra-tion via Virk

DIGITALISERINGSSTYRELSEN

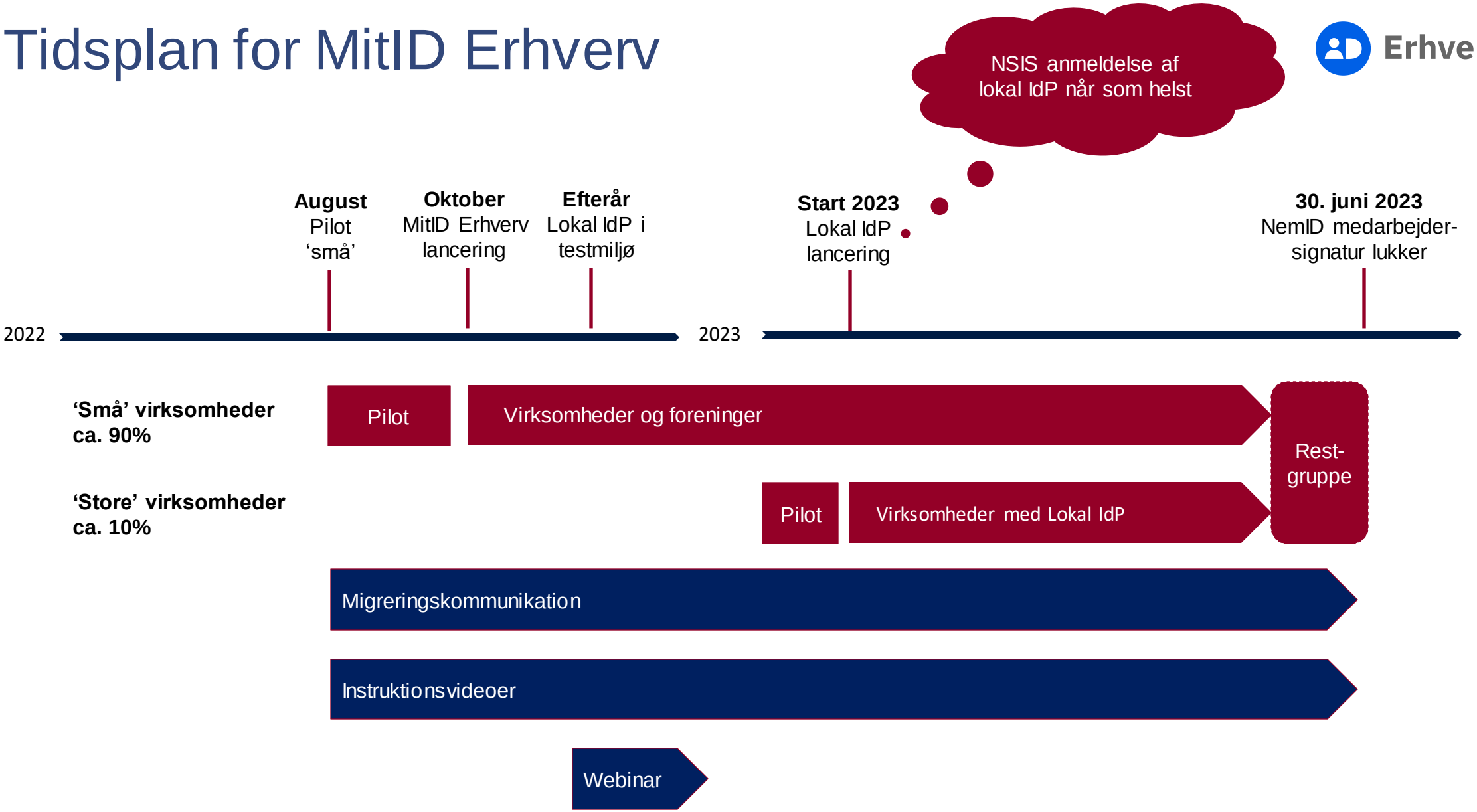
Intro til MitID Erhverv

- MitID Erhverv er afløseren for NemID Erhverv:
  - Samler administration af erhvervsbrugere, rettigheder og fuldmagter ét sted.
  - Understøtter både små og store organisationer.
- MitID Erhverv er en del af NemLog-in løsningen. Første del er gået live i okt. 2022:
  - Første del fokuserer på de mindre brugerorganisationers behov.
  - Anden del giver understøttelse af lokal IdP og er planlagt til primo 2023.
- MitID Erhverv er ikke længere centreret om medarbejdercertifikater:
  - Certifikater kan oprettes for dem, som har et bagudrettet eller internt behov, men man kan ikke logge ind med dem i NemLog-in.
- Øget sikkerhedsniveau:
  - Baseret på NSIS.
  - MitID identifikationsmidler er stærkere end NemID identifikationsmidler.

Migrering af brugerorganisationer

- Brugerorganisationer kan migrere deres eksisterende brugere fra NemID Erhverv til MitID Erhverv og således beholde bl.a. RID-nummer og rettigheder.
- Værktøj til ”massemigrering” kommer primo 2023.
  - Prototype vises senere i præsentationen.
- MitID Erhverv understøtter synkronisering af brugere med en lokal IdM-løsning via IdM API.

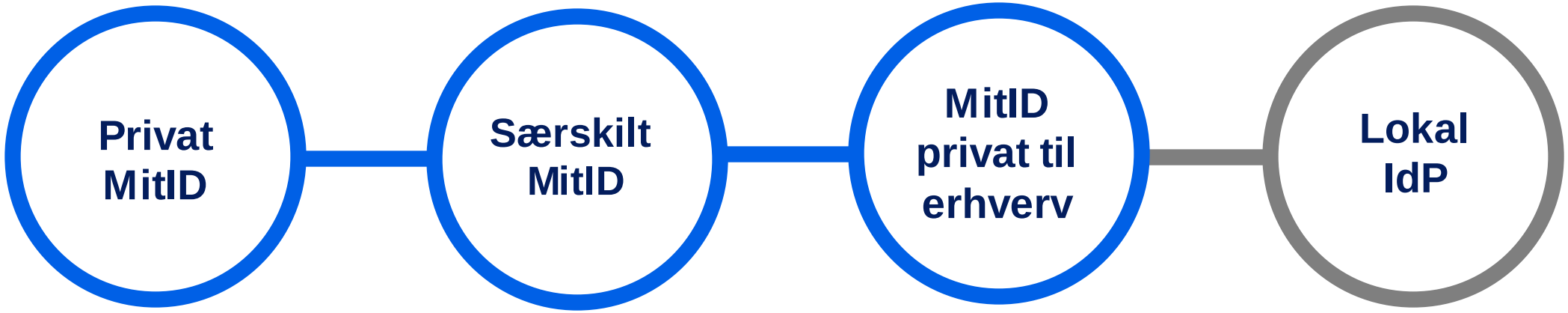
Tidsplan for MitID Erhverv



DIGITALISERINGSSTYRELSEN

Erhvervsidentiteter og identifikationsmidler

Erhverv



Medarbejder bruger sit private MitID til både privat og erhverv.

Kræver samtykke fra begge parter.

Det dobbelte frivillighedsprincip.

Medarbejder bruger sit private MitID til privat og et andet MitID til erhverv.

Kun til erhvervsbrug.

Hvis én af parterne ønsker det.

Person, der er fuldt ansvarlig deltager, bruger sit private MitID til både privat og erhverv.

Svarer til "NemID privat til erhverv".

Særlig mulighed for visse virksomheder og foreninger.

Medarbejder bruger sit private MitID til privat og et andet ID-middel til erhverv.

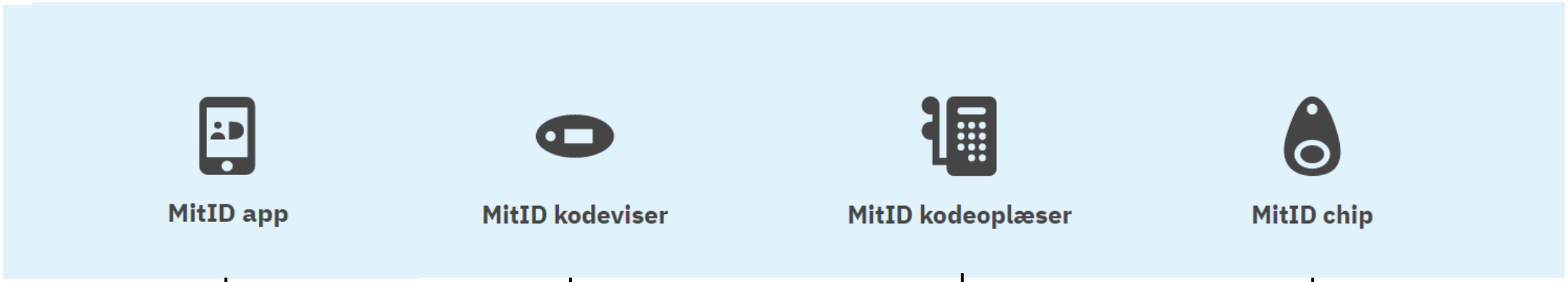
Udstedt af Lokal IdP.

Kun hvis virksomheden vælger Lokal IdP.

DIGITALISERINGSSTYRELSEN

MitID identifikationsmidler

Erhverv



Med et swipe på din mobiltelefon eller tablet kan du logge ind og godkende med MitID på vegne af din virksomhed eller forening.

Du kan anvende den MitID app, du har på din private telefon eller tablet. Eller du kan få en særskilt MitID app til erhvervsbrug på fx din arbejdstelefon.

MitID kodeviseren er en lille, elektronisk enhed, der viser en engangskode, når du trykker på en knap.

MitID kodeoplæser er beregnet til personer med nedsat syn. Den viser og læser en unik engangskode højt.

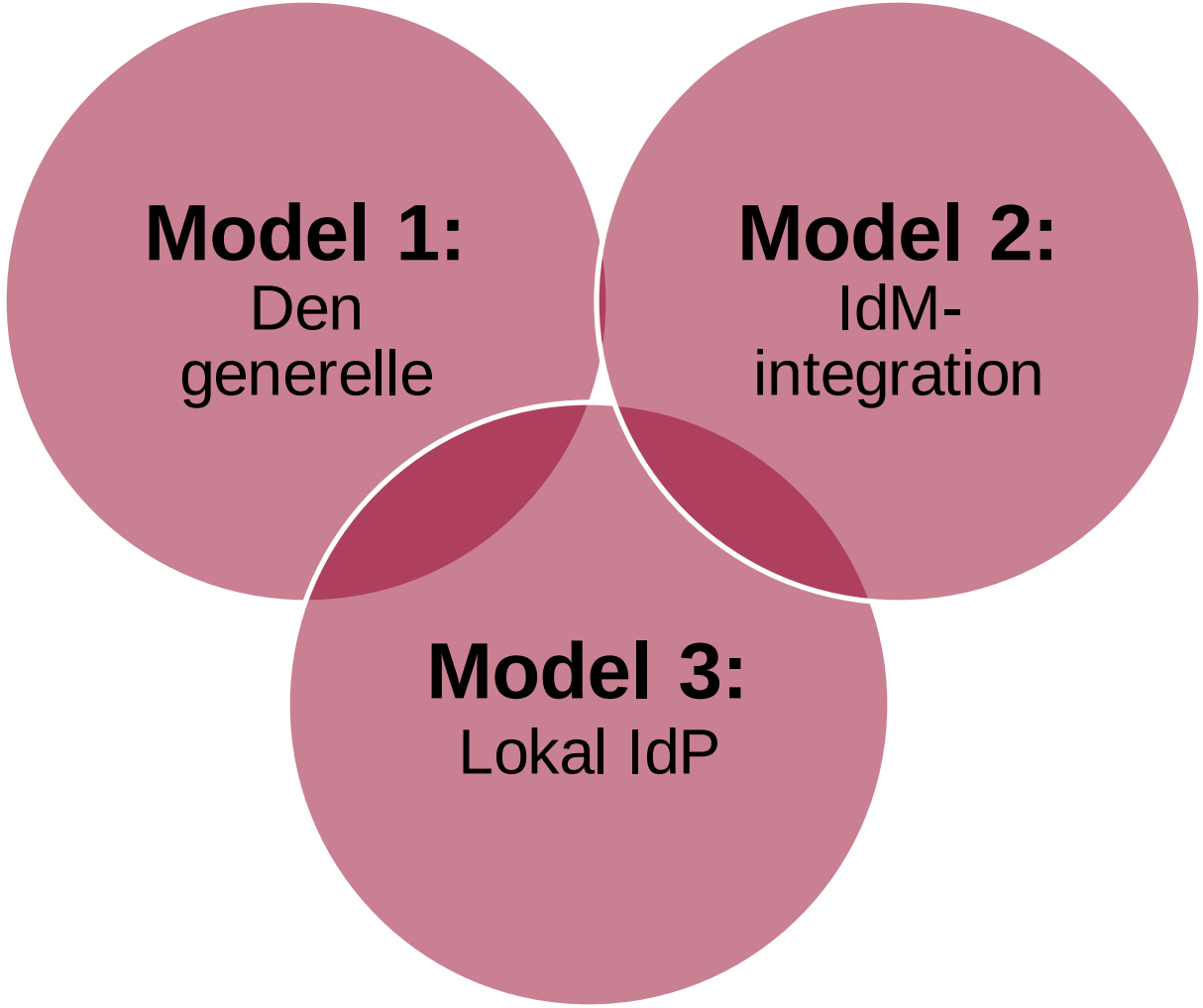
MitID chip er til dig, der har brug for at godkende og logge på med MitID mange gange hver dag, fx i forbindelse med dit arbejde.

DIGITALISERINGSSTYRELSEN

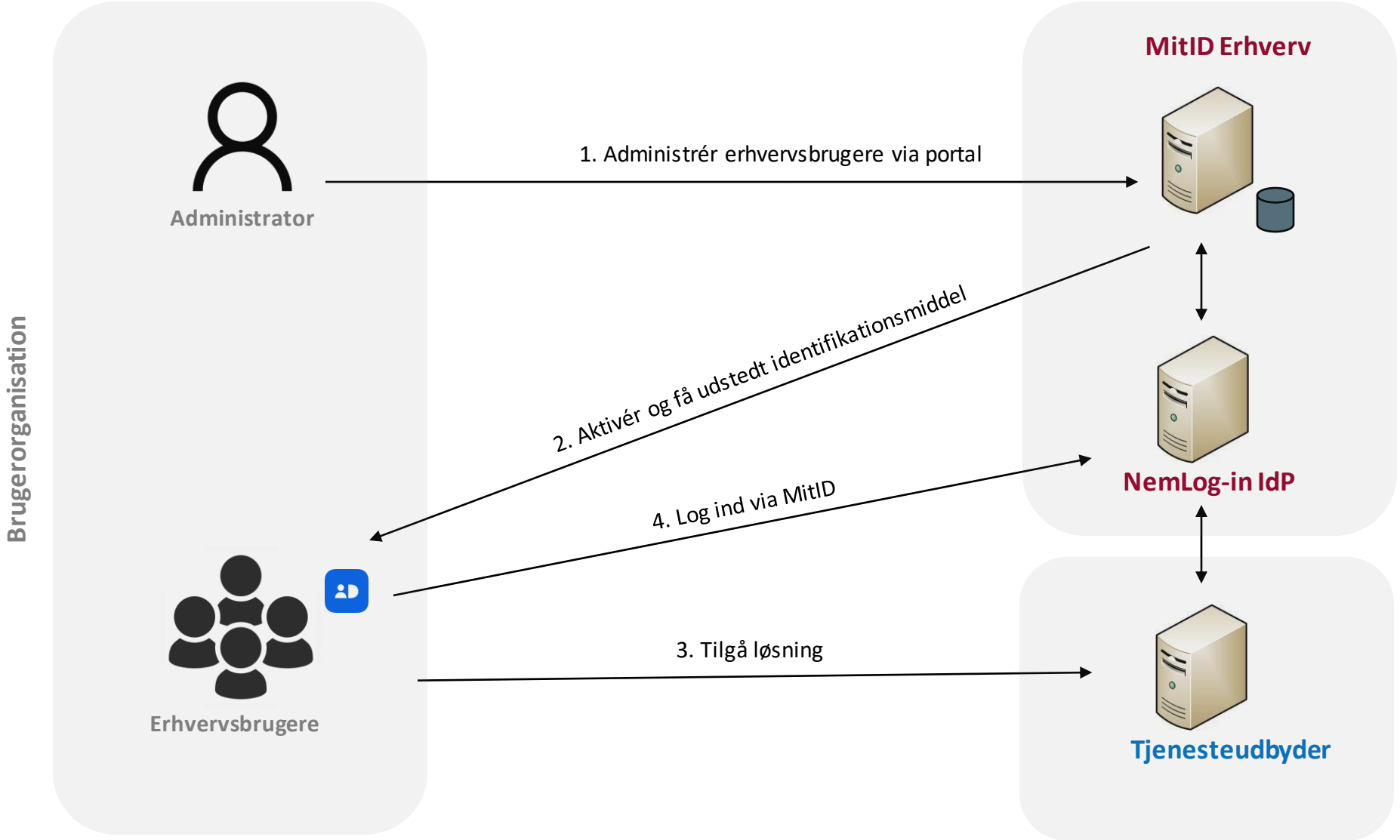
Tre modeller for anvendelse af MitID Erhverv

Tre modeller for anvendelse af MitID Erhverv

- Man behøver ikke følge samme model for alle brugere i organisationen



Model 1 – Den generelle: Ren central model



Model 1 – Den generelle: Ren central model

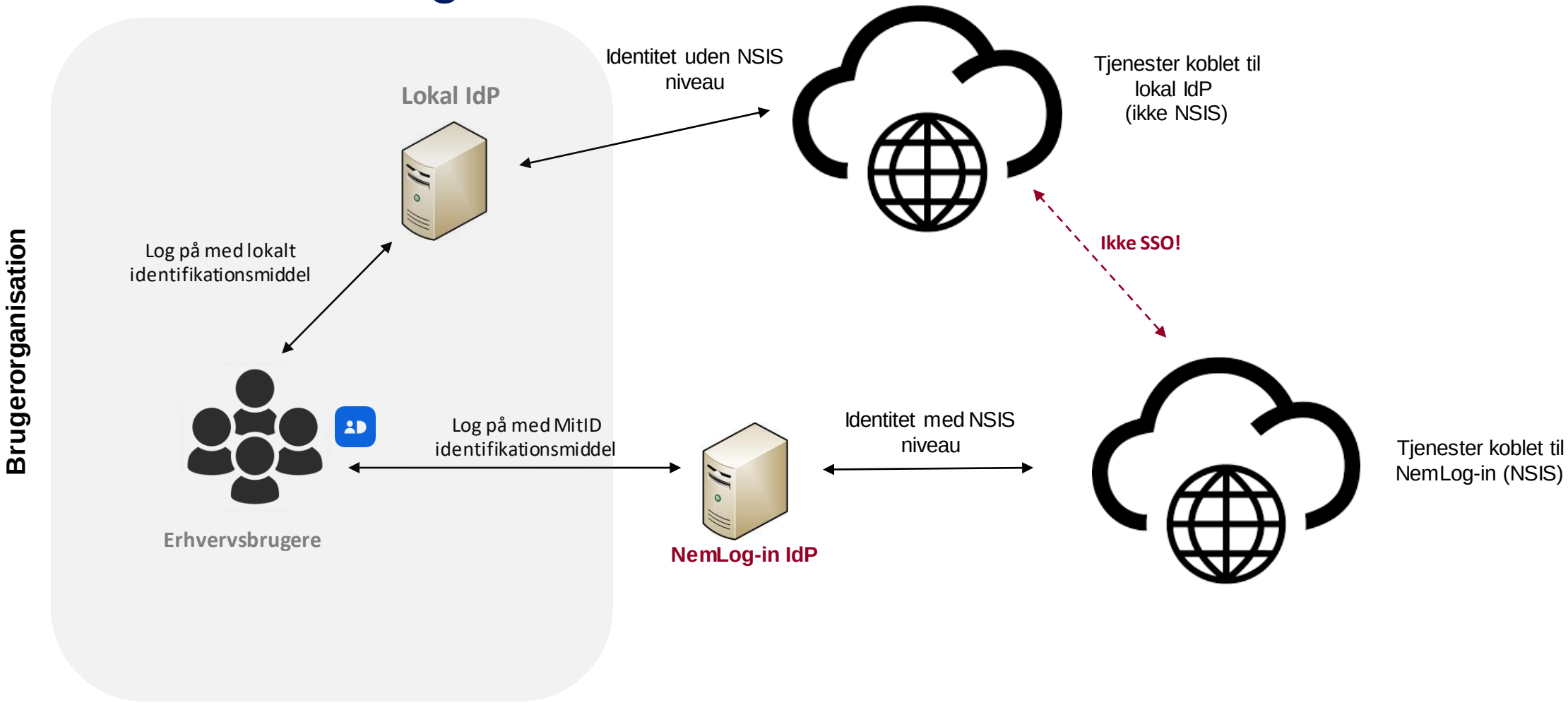
Erhverv

- Benytter den centrale MitID Erhverv-løsning som 'totalløsning' ved at importere identiteter fra NemID Erhverv.
- Brugerne kan enten få udstedt nyt MitID identifikationsmiddel (app, kodeviser, chip) eller benytte deres private MitID identifikationsmiddel til deres erhvervsidentitet (dobbelt frivillighedsprincip).
- Fordele:
  - Ikke behov for at etablere lokal IdP (eller NSIS-anmelde en lokal IdP man allerede har).
  - Brugerne kan signere med kvalificerede signaturer 'out-of-the-box'.
  - Ingen NSIS anmeldelse for brugerorganisationen – NSIS håndteres af MitID Erhverv.
- Ulemper:
  - Brugerne med behov for MitID Erhverv skal administreres 'ved håndkraft' i MitID Erhverv portalen.
  - Slutbrugerne får et ekstra bruger-ID og et ekstra identifikationsmiddel (hvis de ikke genbruger deres private).
  - Slutbrugerne skal potentielt logge ind flere gange, når de tilgår løsninger i adskilte føderationer (se næste slide).

DIGITALISERINGSSTYRELSEN

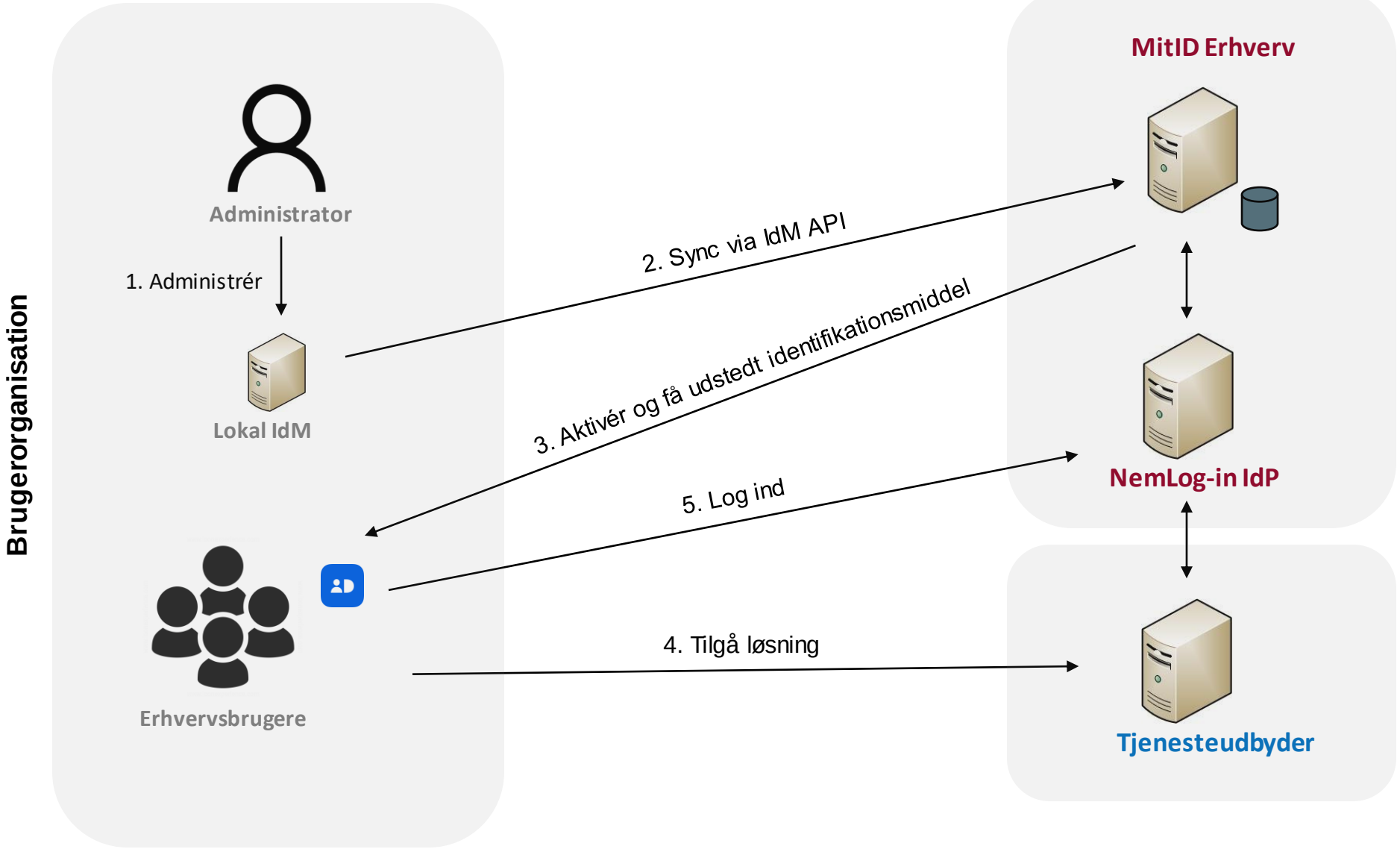
Model 1 – Den generelle: To 'øer' uden SSO

Erhverv



DIGITALISERINGSSTYRELSEN

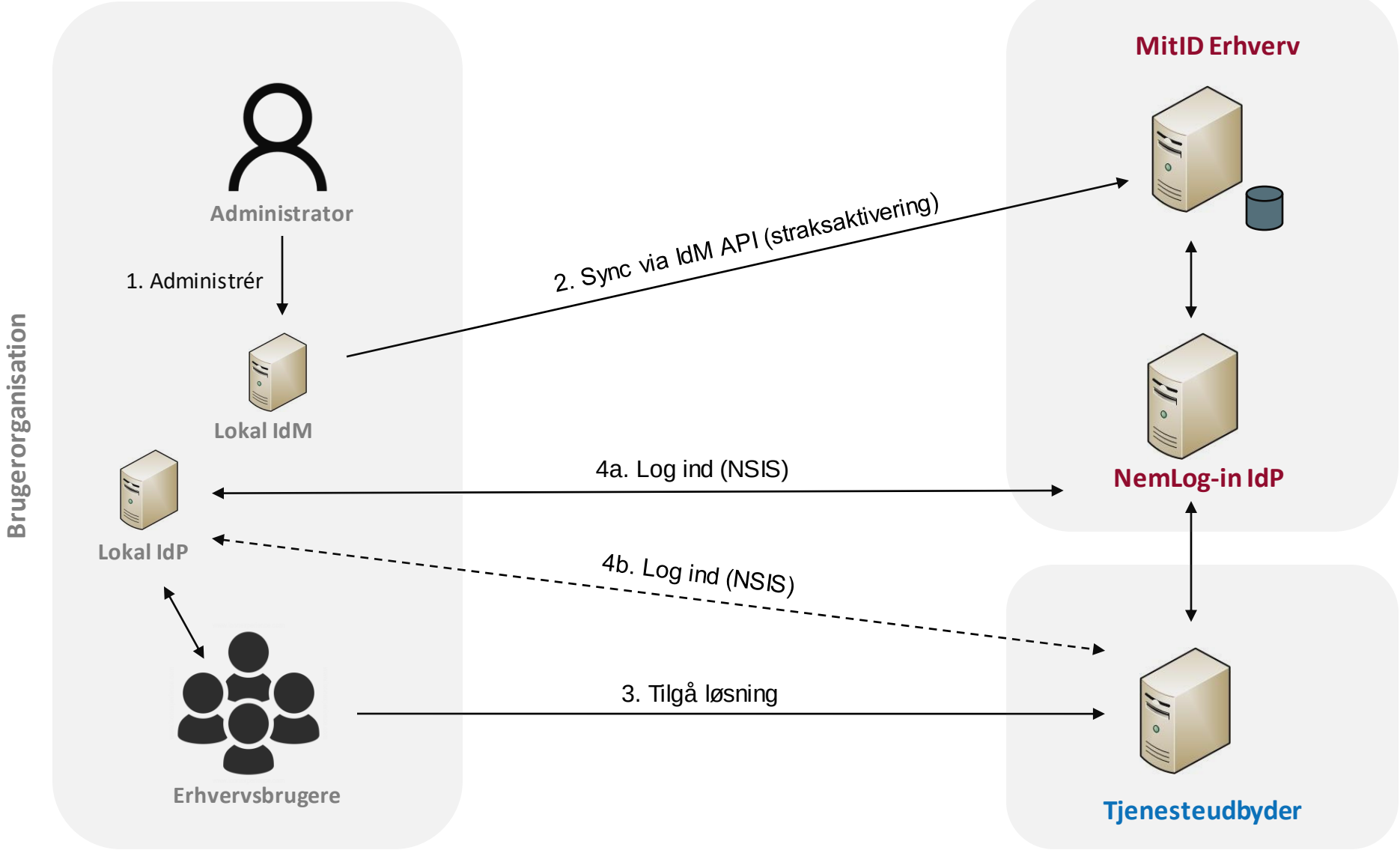
Model 2 – IdM integration: API i stedet for UI



Model 2 – IdM integration: Kombineret central / decentral model

- Benytter den centrale MitID Erhverv-løsning, men føder den lokalt:
  - Brugerne administreres lokalt i egen løsning og synkroniseres ind i MitID Erhverv via API-integration.
    - Alternativ til administration via brugergrænseflade.
  - MitID Erhverv sørger for brugeraktivering og udstedelse af MitID identifikationsmiddel.
- Brugerne kan enten få udstedt nyt MitID identifikationsmiddel (app, kodeviser, chip) eller benytte deres private MitID identifikationsmiddel med deres erhvervsidentitet (dobbelt frivillighedsprincip).
- Fordele:
  - Mere effektiv brugeradministration.
  - Ikke behov for at etablere lokal IdP (eller udvide en lokal IdP man allerede har).
  - Brugerne kan signere med kvalificerede signaturer 'out-of-the-box'.
  - Ingen NSIS anmeldelse for organisationen – NSIS håndteres af MitID Erhverv.
- Ulemper:
  - Integration med IdM API.
  - Slutbrugerne får et ekstra bruger-ID og et ekstra identifikationsmiddel (hvis de ikke genbruger deres private).
  - Slutbrugerne skal potentielt logge ind flere gange, når de tilgår løsninger i adskilte føderationer.

Model 3 – Lokal IdP: Lokal NSIS-anmeldt IdP



Model 3 – Lokal IdP: Lokal NSIS-anmeldt IdP

Erhverv

- Brugerorganisation vælger at benytte sin egen lokale IdP løsning og styre alle aspekter vedrørende brugerne selv.
- Brugerne har ikke behov for at få udstedt MitID identifikationsmidler til erhvervsbrug.
- Fordele:
  - Slutbrugerne får ikke ekstra bruger-ID'er og identifikationsmidler.
  - Single sign-on på tværs af alle løsninger koblet til den lokale IdP og NemLog-in.
  - NSIS anmeldt lokal IdP kan være et krav i andre føderationer, så man slår flere fluer med ét smæk.
- Ulemper:
  - Den lokale IdP skal NSIS anmeldes og årligt revideres af en statsautoriseret revisor.
  - Brugerne kan ikke signere med kvalificerede signaturer 'out-of-the-box'.
    - Skyldes eIDAS forordningens artikel 24.1.
    - Kræver aktivering (identitetssikring) af erhvervsidentitet med privat MitID.

DIGITALISERINGSSTYRELSEN

Model 3 – Lokal IdP: Detaljer

- Brugerne skal synkroniseres til MitID Erhverv også ved brug af lokal IdP:
  - Alle brugeridentiteter, som autentificeres via lokal IdP, skal være oprettet i MitID Erhvervs centrale database.
  - Når den lokale IdP autentificerer en bruger, skal Subject i SAML Assertion udpege en entydig brugeridentitet for brugerorganisationen i MitID Erhverv.
  - En bruger kan godt have flere identiteter i MitID Erhverv og lokalt vælge (ved lokal autentifikation) hvilken identitet, der benyttes.
  - Priser:
    - En lokal bruger koster således også 20 kr., da brugeren skal oprettes centralt i MitID Erhverv. (https://digst.dk/it-loesninger/nemlog-in/priser/).
    - Det er dog gratis at migrere eksisterende brugere fra NemID til MitID Erhverv.
    - De første tre brugere er gratis som hidtil.

Model 3 – Lokal IdP: Guide til etablering

Erhverv

Afklar ønsker og behov, fx NSIS sikringsniveau og integration.

Etabler projekt, og skab ledelsesopbakning.

Sammenhold NSIS krav med nuværende processer og systemer.

Implementér nødvendige systemer og processer.

Foretag testtilslutning mod NemLog-in, og afprøv lokal IdP i integrationstestmiljø.

Indhent revisionserklæringer og ledelseserklæringer til NSIS-anmeldelse.

Indsend anmeldelsespakke til Digitaliserings-styrelsen.

Kontakt NemLog-in forvaltning, og bed om rettighed til oprettelse af lokal IdP.

Tilslut lokal IdP til produktionsmiljø.

Hent guiden på www.nemlog-in.dk

DIGITALISERINGSSTYRELSEN

Gør klar til MitID Erhverv

Sådan gør I klar til MitID Erhverv

Erhverv

1. Beslut, hvordan I vil anvende MitID Erhverv jf. de tre modeller.
2. Ryd op i brugere og administratorer i NemID medarbejdersignatur og Brugeradministrationen.
3. Opdatér kontaktoplysninger på NemID superadministrator i NemID medarbejdersignatur.
4. Opdatér ledelse i CVR.
5. Beslut, hvem der skal gennemføre tilslutning, og hvem der skal være administratorer i MitID Erhverv.
6. Tag stilling til, hvordan jeres erhvervsbrugere skal logge ind med MitID.
7. Test, om jeres integrationer og egne løsninger fungerer med de nye certifikattyper. Hav særlig opmærksomhed på identifikatorer og algoritmer.

- Generel
- IdM integration
- Lokal IdP

Læs mere på:
Gør din organisation klar - Nemlog-in

DIGITALISERINGSSTYRELSEN

Spørgsmål

DIGITALISERINGSSTYRELSEN

Masseadministration af importerede brugere

Importerede brugere

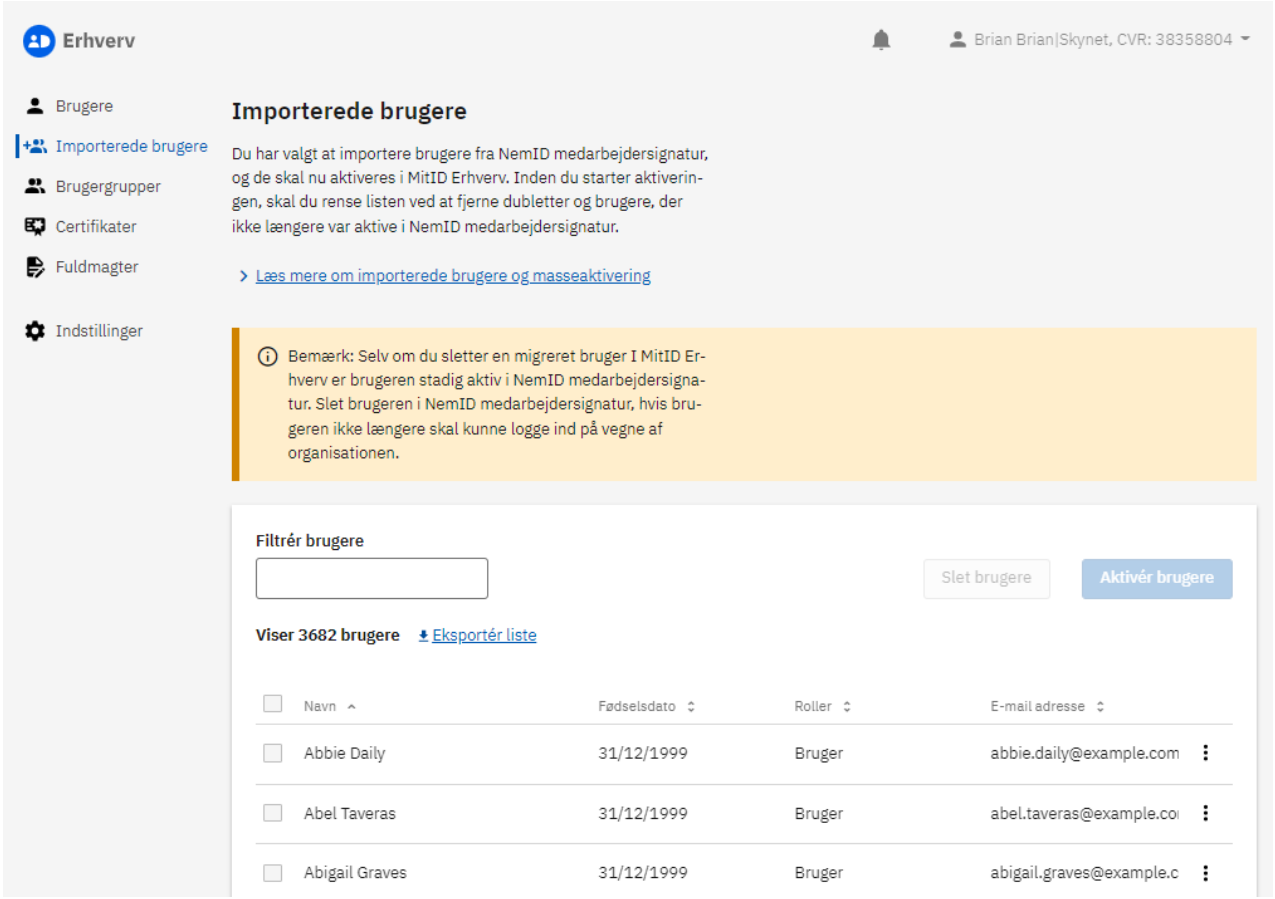
- Brugere hentes fra NemID medarbejdersignatur med deres RID og oprettes i MitID Erhverv sammen med et nyt UUID.
- Importerede brugere skal aktivere sig og have identifikationsmiddel for at kunne logge ind.
  - De vil have samme rettigheder som i NemID Erhverv, da RID er bibeholdt.
- En importeret bruger, der eksisterer (nøgle: RID) i den gamle Brugeradministration (FBRS), kan ikke længere slettes gennem brugergrænsefladen i FBRS, kun ses.
  - Brugeren kan stadig logge ind på tjenester med NemID Erhverv.

Masseadministration af importerede brugere

Importerede brugere fra NemID erhverv kan administreres samlet.

Opgaver:

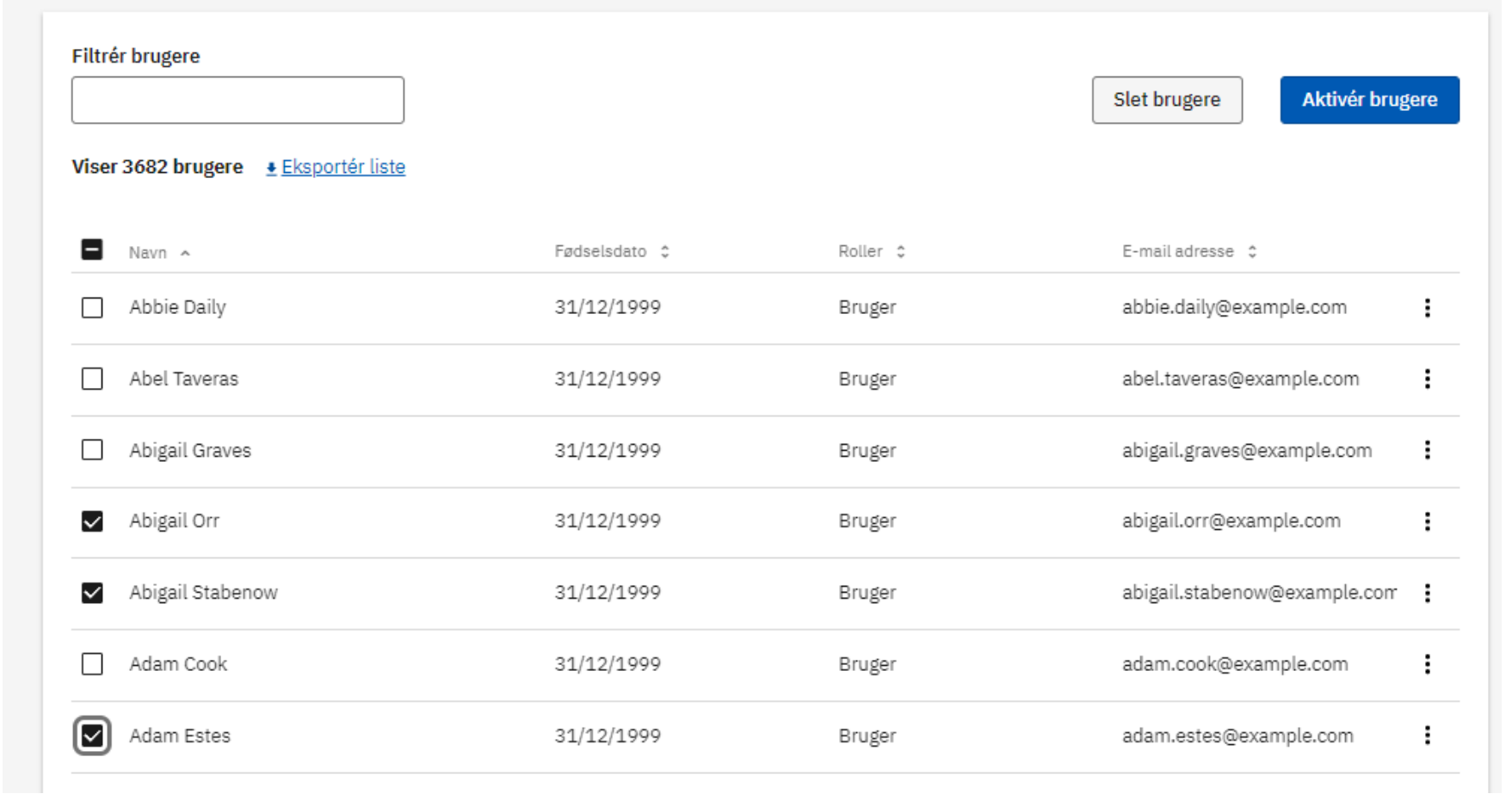
- Oprydning (også i NemID Erhverv)
- Fødselsdag / CPR er påkrævet
- Aktivering via:
  - NemID medarbejdersignatur (hvis ikke CPR angives)
  - Privat MitID / NemID.



DIGITALISERINGSSTYRELSEN

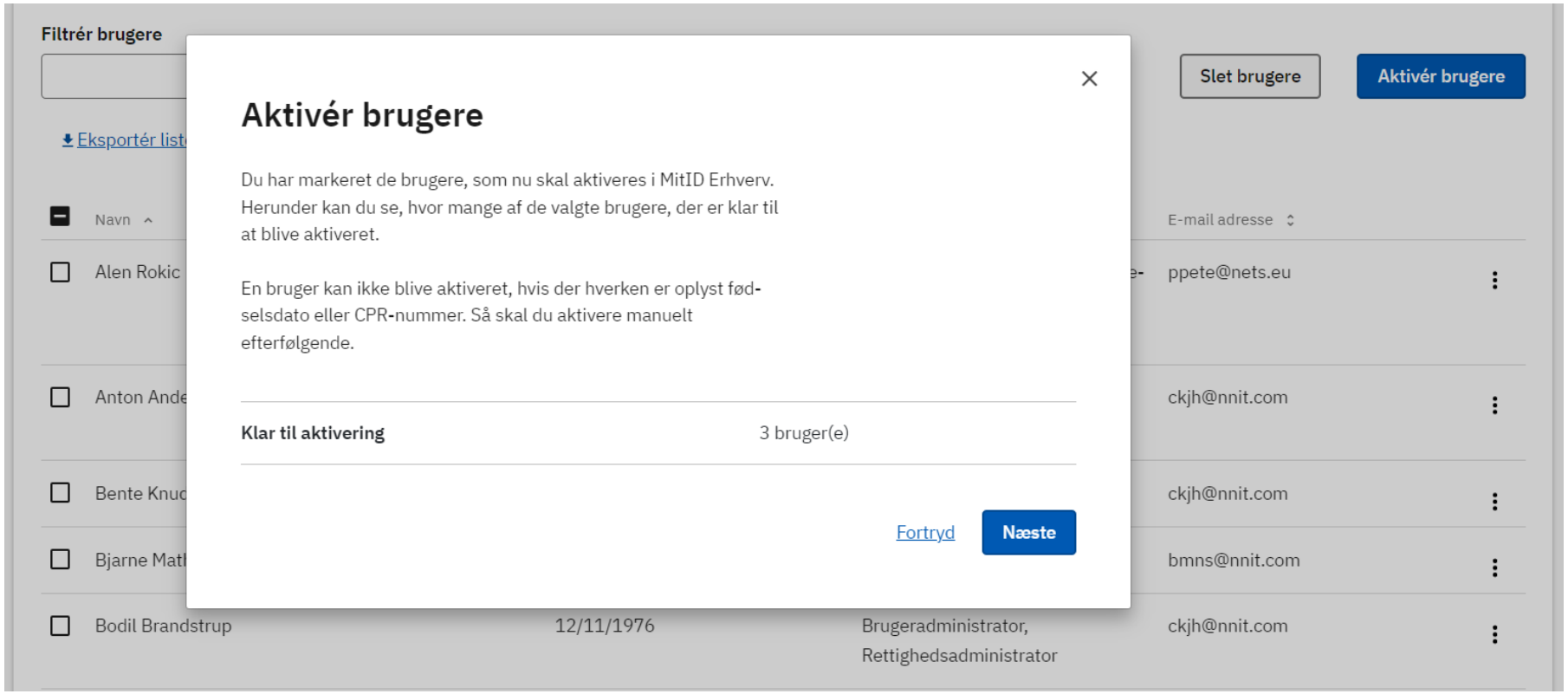
Vælg brugere til aktivering

Erhverv

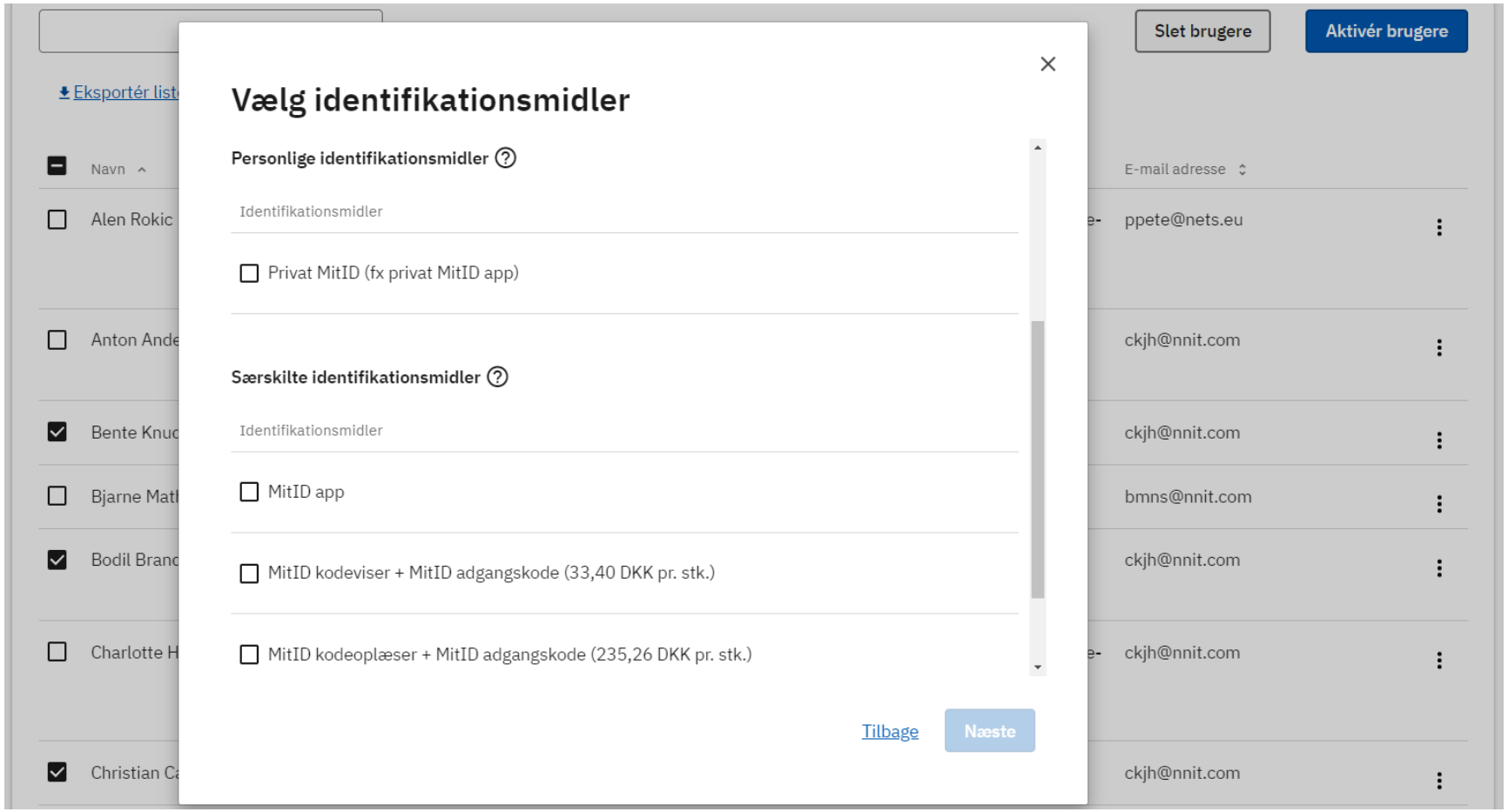


DIGITALISERINGSSTYRELSEN

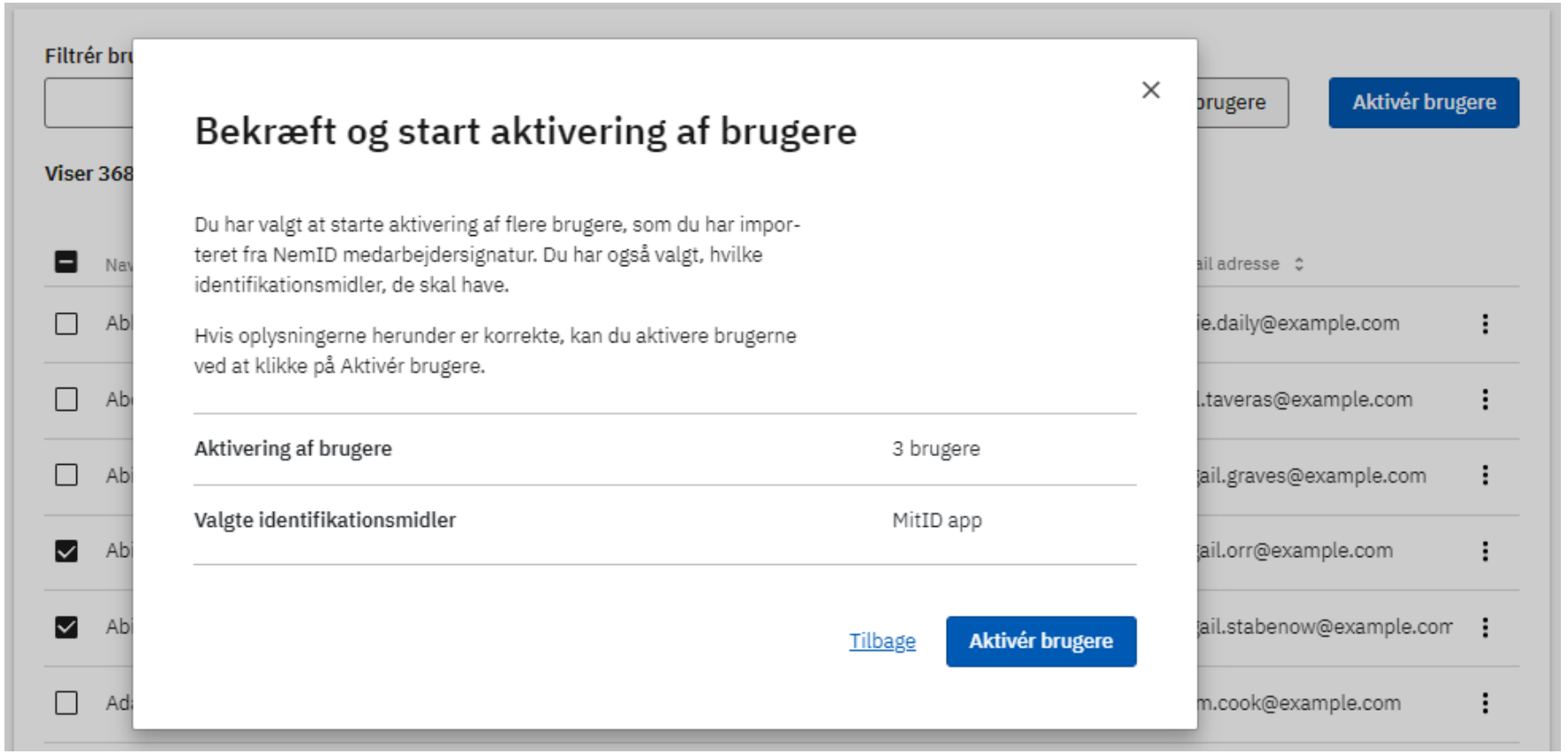
Aktivering


Filtrér brugere
Slet brugere
Aktivér brugere
Eksportér list
Navn
E-mail adresse
Alen Rokic
ppete@nets.eu
Anton Ande
ckjh@nnit.com
Bente Knud
ckjh@nnit.com
Bjarne Matl
bmns@nnit.com
Bodil Brandstrup
12/11/1976
Brugeradministrator, Rettighedsadministrator
ckjh@nnit.com
Aktivér brugere
Du har markeret de brugere, som nu skal aktiveres i MitID Erhverv. Herunder kan du se, hvor mange af de valgte brugere, der er klar til at blive aktiveret.
En bruger kan ikke blive aktiveret, hvis der hverken er oplyst fødselsdato eller CPR-nummer. Så skal du aktivere manuelt efterfølgende.
Klar til aktivering
3 bruger(e)
Fortryd
Næste

Vælg identifikationsmidler



Bekræft og start aktivering (mails sendes)



IdM-integration og Lokal IdP

Integration med nye erhvervsidentiteter

Erhverv

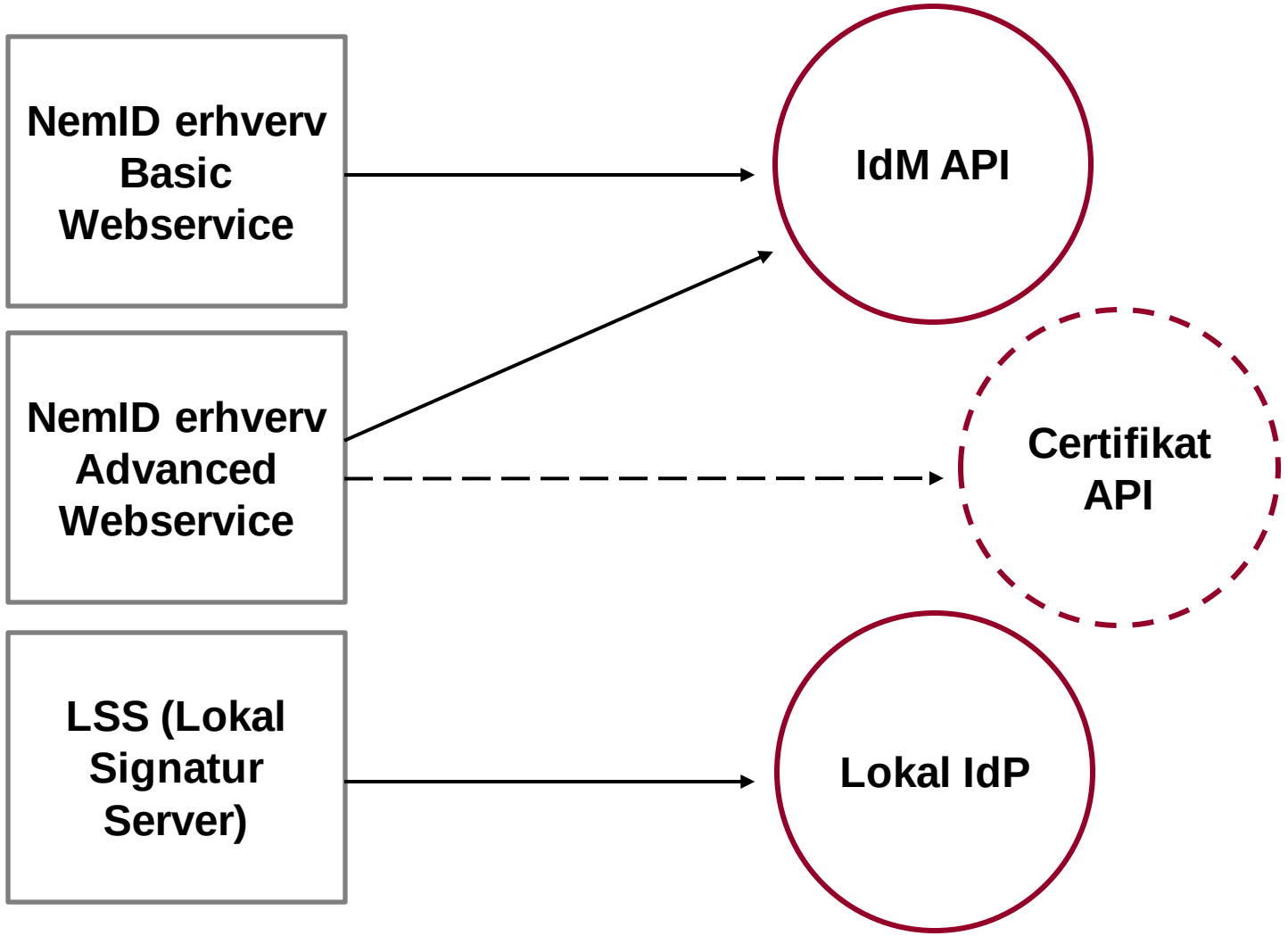
IdM API

- API stilles til rådighed til administration af erhvervsidentiteter og rettigheder.
- Primært til brug fra egne Identity Management systemer som fx Microsoft AD.
- Mulighed for 3. part udvikling af løsninger.

Lokal IdP

- Organisationens egen Identity Provider, fx Microsoft ADFS, kan integreres til MitID Erhverv.

NemID vs. MitID Erhverv løsninger



IdM-integration

Muligheder med API

- IDM API - Administration af brugere:
  - Opret
  - Slet
  - De-aktivering (evt. i periode)
  - Tildel rettigheder
  - Håndtering af identifikationsmidler
- Certifikat API (EST)
  - Medarbejdercertifikater
  - Virksomheds- og System-certifikater.

- SOAP og REST understøttes.

REST services - OpenAPI / swagger

Erhverv

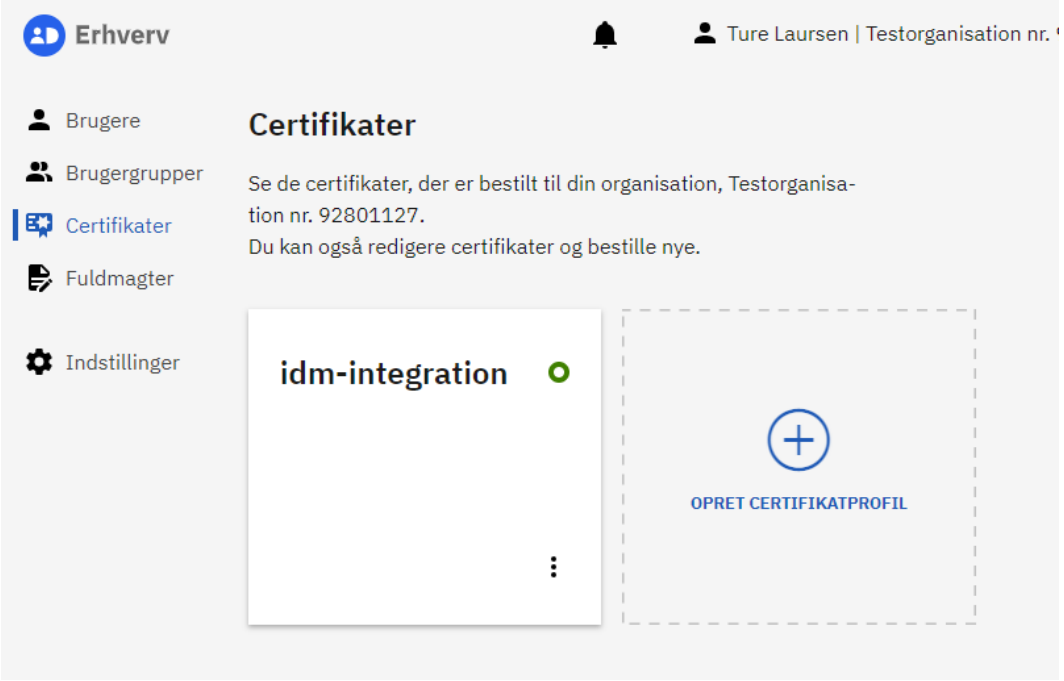
- IDM API pakken indeholder v1.yaml, der beskriver REST interfacet.
  - Kan importeres med swagger codegen eller andet udviklingsværktøj, fx https://editor.swagger.io.
  - C# .Net 6 kodeeksempel er inkluderet i pakken.
- Centrale services:
  - IDMLoginService – interfacet til autentifikation med klientcertifikat.
  - EmployeeIdentityService – administration af brugere, rettigheder, identifikationsmidler.
  - OrganizationService – stamdata på aktuel organisation, p-numre, godkendt IAL-niveau m.m.
  - OrganizationRightsService - tilgængelige rettigheds-roller, grupper, fuldmagter for organisationen.
  - ValuesService – bl.a. tilgængelige identifikationsmidler opsat af organisationen.

  - ESTService – certifikatudstedelse via EST standarden.
  - CertificateService, CertificateOrderService - bestilling og håndtering af certifikater udover EST.

DIGITALISERINGSSTYRELSEN

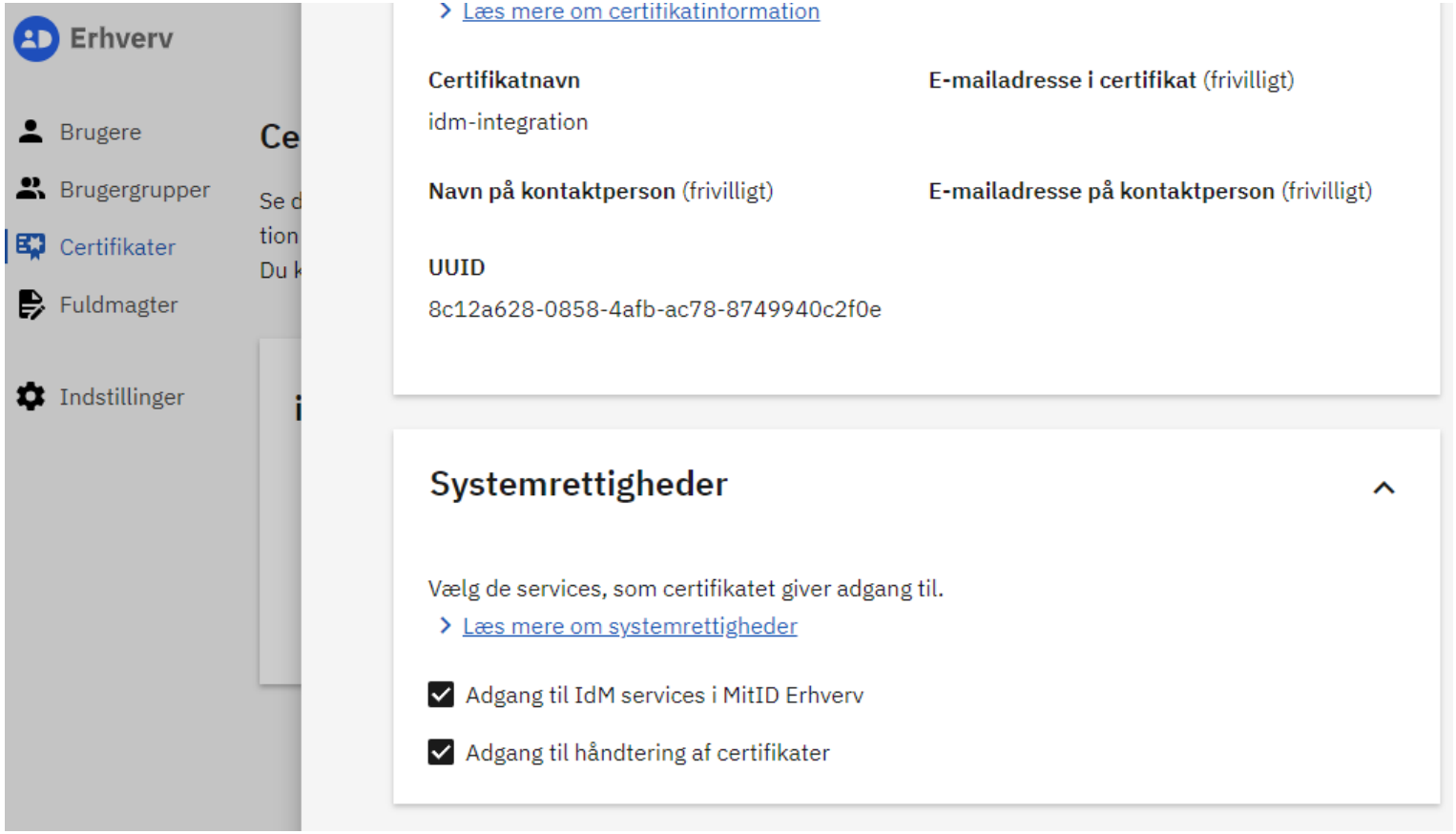
Autentifikations-model, IDM API

- Autentifikation sker med system-certifikat som klient-certifikat.
- Organisationer skal godkendes af Digitaliseringsstyrelsen til at bruge IDM API, før de selv kan tildele rettighed til certifikat-profil.
- Certifikater udstedt under den autoriserede certifikat-profil vil have adgang til API.



Autentifikationsmodel

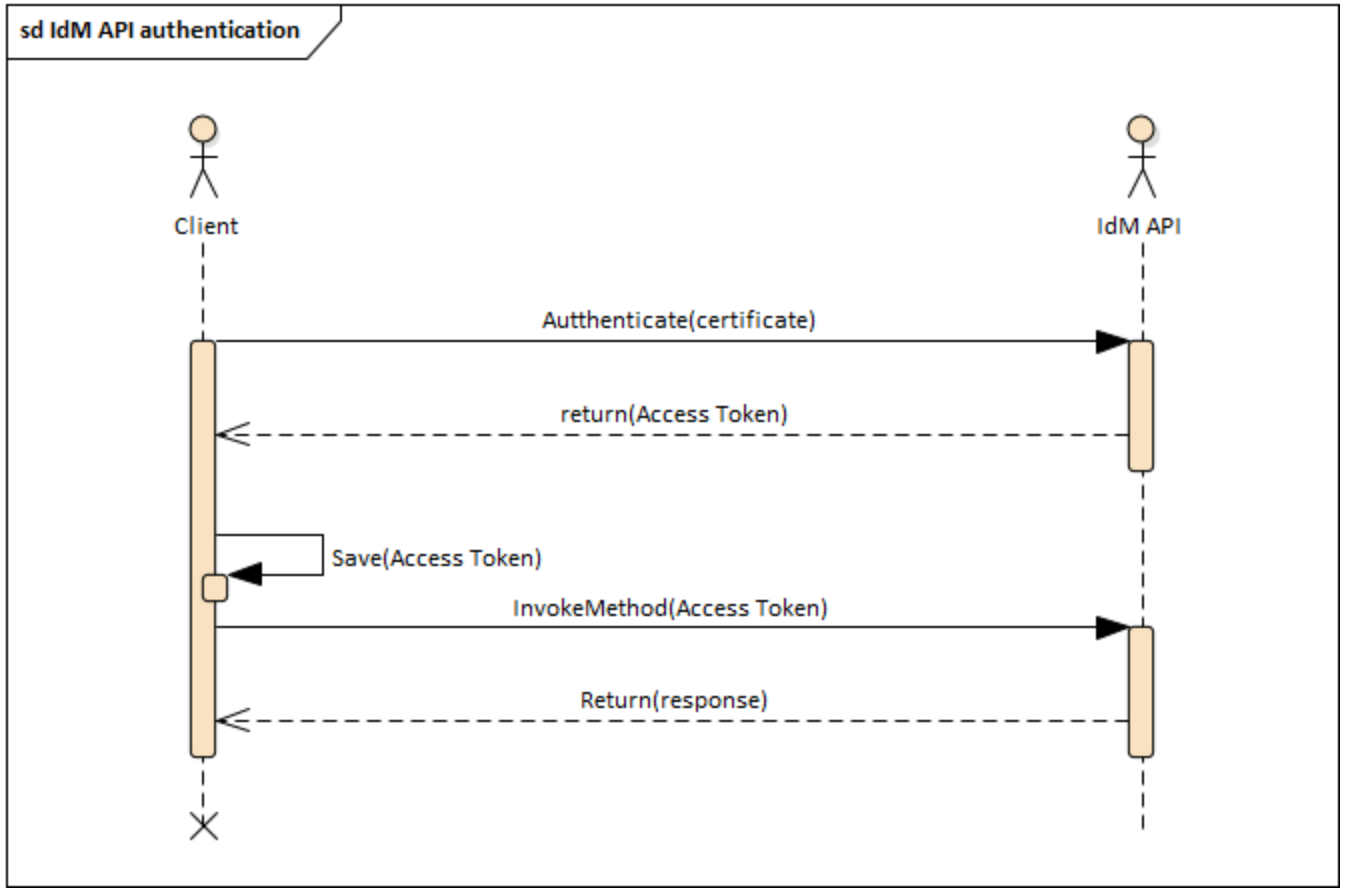
- Certifikat-profilen kan tildeles adgang til IDM og Certifikat API uafhængigt.
- Certifikater udstedt under denne certifikat-profil vil have adgang.



Veksling til access token

JWT access tokens hentes via: POST /api/administration/idmlogin/tls/authenticate

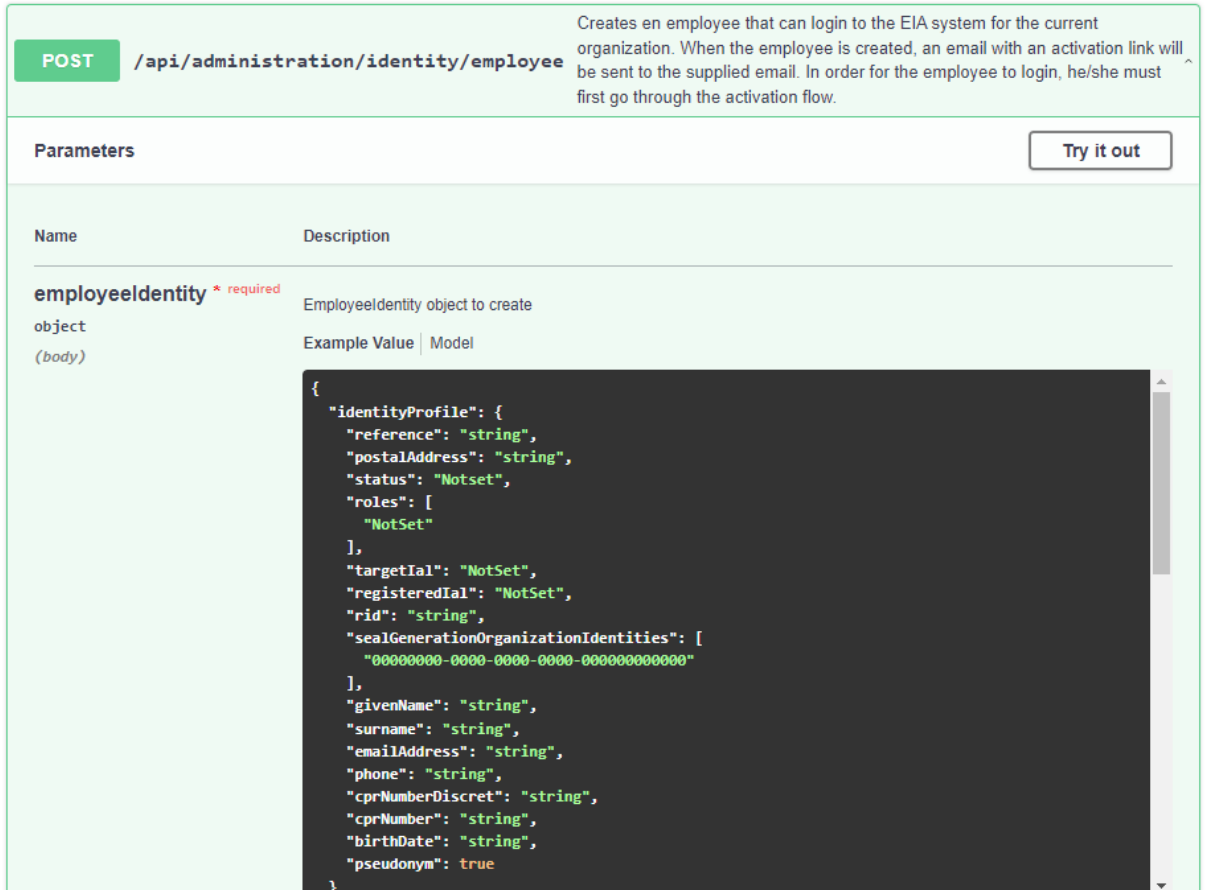
De bruges i efterfølgende API kald som bearer token.



Opret bruger

Erhverv

- Fulde navn, som i CPR.
- CPR eller fødselsdato (+ engangskode).
- Evt. RID, hvis FBRS rettigheder skal beholdes.
- Identifikationsmidler:
  - Privat MitID / NemID
    - Bruger skal godkende brug.
    - Aktiveringsflow kan undgås, hvis CPR angives.
  - Særskilt MitID identifikationsmiddel
    - App, CodeDisplay, CodeReader, U2FToken.
    - Bruger skal gennem aktiveringsflow.
  - Lokal IdP (authenticator LocalIdentityProvider)
    - EmployeeAuthenticatorDataCreate.subjectNameId.
    - Ikke noget aktiveringsflow.
- Rettigheder:
  - identityPermissions.roleAssignments, groupAssignments.

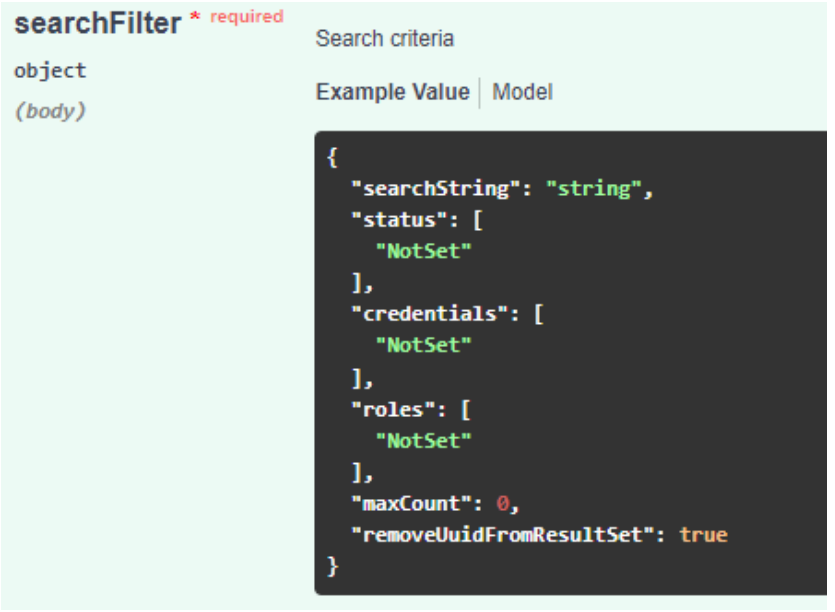


DIGITALISERINGSSTYRELSEN

Søgning

Erhverv

Eksempel fra IDM API dokumentations-pakken (C# .Net 6)



POST /api/administration/identity/employee/search

```
private static void SearchIdentities(string? searchPhrase)
{
    var eSearch = new EmployeeSearchFilter
    {
        // We will look for active and pending users
        Status = new List<Status> { Status.Active, Status.ActivationPending },
        // SearchString will search for match in Givenname, Surname, Emailaddress and,
        // if 10 digits are supplied, also CPR
        SearchString = searchPhrase
    };
    var emps = _idm.EmployeeIdentityService_SearchAsync(eSearch, CancellationToken.None).GetAwaiter().GetResult();
    Console.WriteLine($"Returned {emps.Count} of {emps.TotalCount}");

    foreach (var emp in emps.Employees)
    {
        Console.WriteLine($"{emp.Uuid}: {emp.Profile.GivenName} {emp.Profile.Surname}");
        Console.WriteLine(JsonConvert.SerializeObject(emp, Formatting.Indented));
    }
}
```


DIGITALISERINGSSTYRELSEN

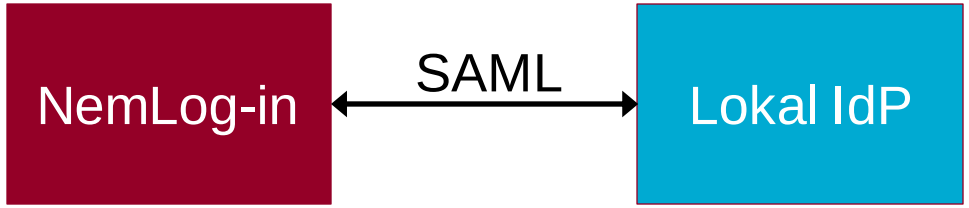
Lokal IdP

Teknisk tilslutning af lokal IdP

- Godkendelse af organisationens NSIS certificering er en forudsætning.
  - Alle kan teste i betatestmiljøet med test-organisation (vælg ”Sikringsniveau for identitetsproces).
- Tilføj lokal IdP i MitID Erhverv:
  - Navn
  - Metadata for den lokale IdP konfiguration
    - Downloades fra serveren hvor IdP er installeret
    - Vælg profil: ADFS / OIOSAML 3
  - Evt. deling med andre CVR-numre.

Teknisk integration, metadata

- Ny SAML-snitflade for Lokal IdP udstilles fra NemLog-in.
- NemLog-in optræder i rollen Service Provider.
- NemLog-in anvender samme certifikat(er) i begge snitflader.
- Eksempler på metadata i det følgende:
  - NemLog-ins Service Provider metadata, som skal registreres hos den Lokale IdP.
  - Metadata for en Lokal IdP, som registreres i MitID Erhverv.



NemLog-in
SP metadata

Erhverv

```
<md:EntityDescriptor
        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://saml.test-devtest4-nemlog-in.dk">
    <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" AuthnRequestsSigned="true" WantAssertionsSigned="true">
        <md:KeyDescriptor>
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certificate>MIIGYjCCB...</X509Certificate></X509Data></KeyInfo>
        </md:KeyDescriptor>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://test-devtest4-nemlog-in.dk/localidp/saml/1.0/" />
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://test-devtest4-nemlog-in.dk/localidp/saml/1.0/" />
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:Kerberos</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat>
        <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://test-devtest4-nemlog-in.dk/localidp/saml/1.0/" index="0" isDefault="true" />
        <md:AttributeConsumingService index="0" isDefault="true">
            <md:ServiceName xml:lang="da">NemLog-in</md:ServiceName>
            <md:RequestedAttribute Name="https://data.gov.dk/model/core/specVersion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true" />
            <md:RequestedAttribute Name="https://data.gov.dk/concept/core/nsis/loa" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true" />
            <md:RequestedAttribute Name="https://data.gov.dk/model/core/eid/professional/cvr" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true" />
            <md:RequestedAttribute Name="https://data.gov.dk/model/core/eid/professional/orgName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true" />
            <md:RequestedAttribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
        </md:AttributeConsumingService>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```


DIGITALISERINGSSTYRELSEN

Lokal IdP metadata

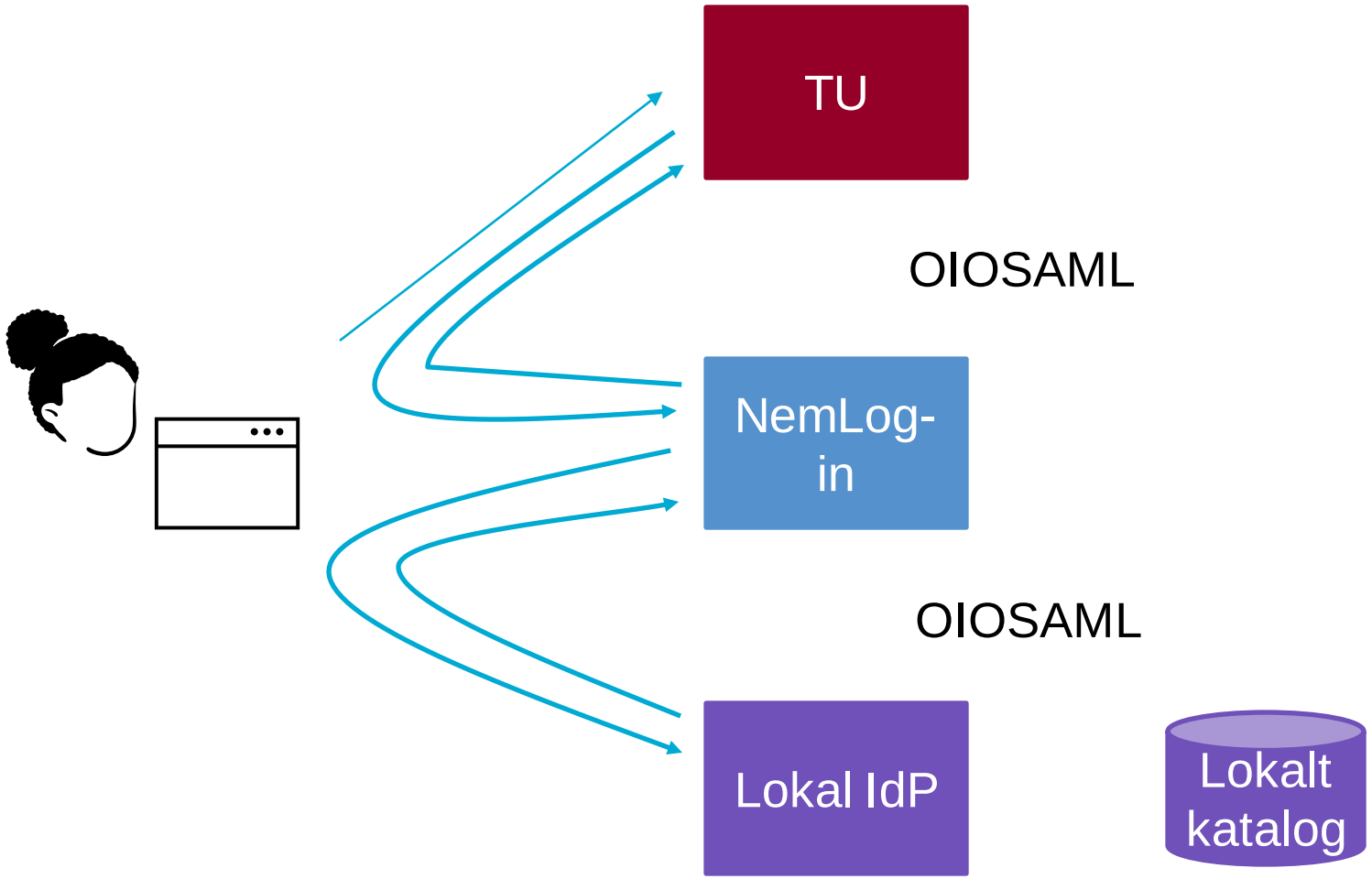
Erhverv

```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ID="_4f022ebe-5055-491f-b0d9-e7c422c98f3c"
   entityID="https://saml.idp.teststrup.dk">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
            MIIGfDCCBLCgAwIBAgIUZ1YmSH0cVIarpR...
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://testlocalidp0.sp-devtest2-nemlog-in.dk/
     SingleLogout/ServiceProvider/" ResponseLocation="https://testlocalidp0.sp-devtest2-nemlog-in.dk/SingleLogout/LogoutResponse/"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://testlocalidp0.sp-devtest2-nemlog-in.dk/
     SingleSignOn/"/>
    <saml:Attribute Name="https://data.gov.dk/model/core/specVersion" FriendlyName="SpecVer" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
     format:uri"/>
    <saml:Attribute Name="https://data.gov.dk/concept/core/nsis/loa" FriendlyName="NSISLevelOfAssurance"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr" FriendlyName="CVR" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
     format:uri"/>
    <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/orgName" FriendlyName="OrganizationName"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    <saml:Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate" FriendlyName="Privileges"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```


DIGITALISERINGSSTYRELSEN

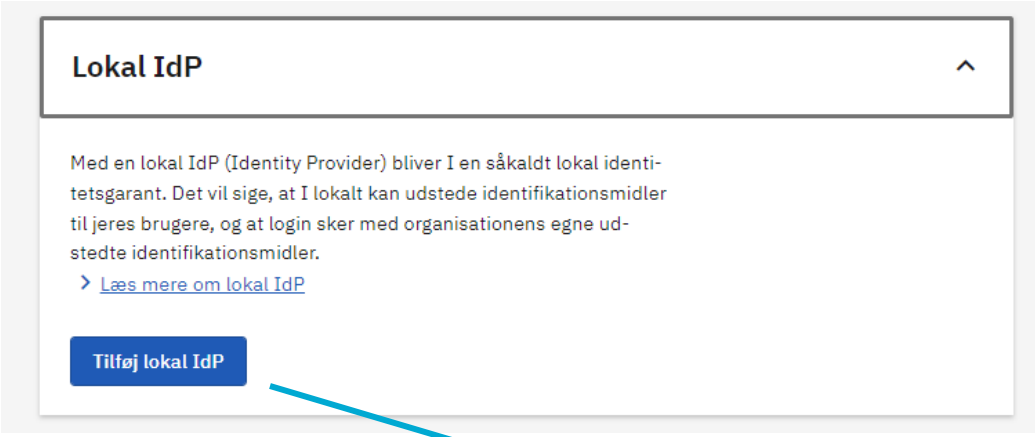
Lokal IdP - anvendelse

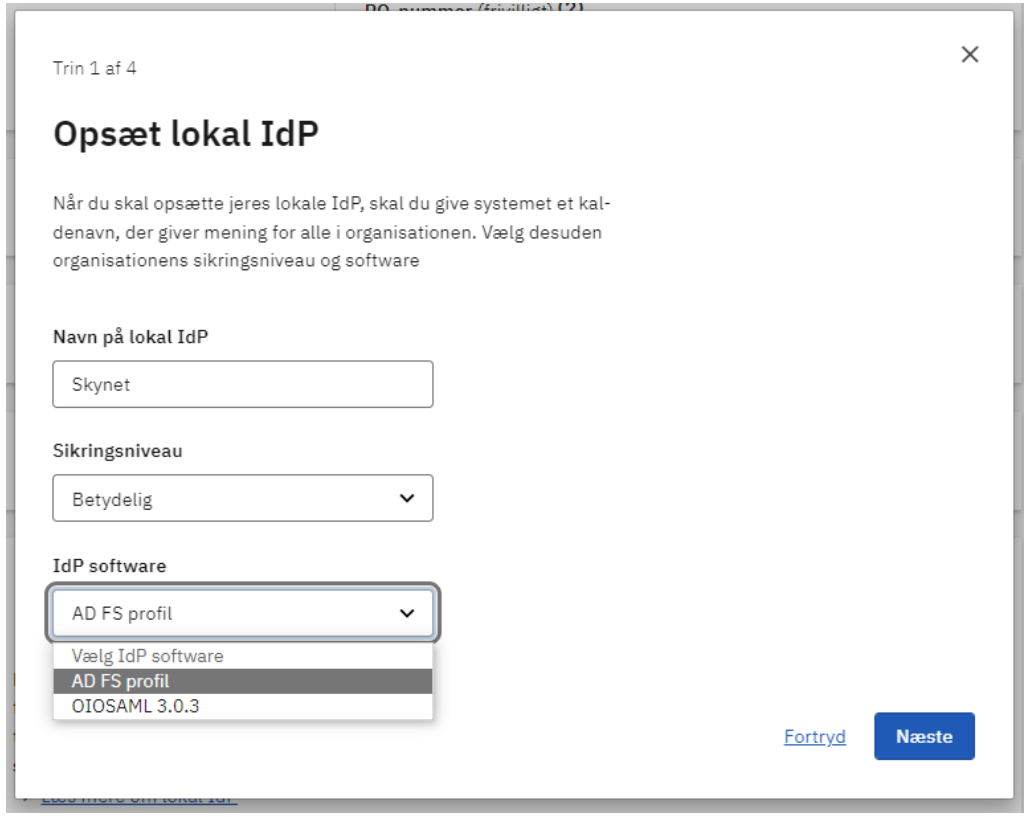
Erhverv



Administrator tilføjer lokal IdP i MitID Erhverv

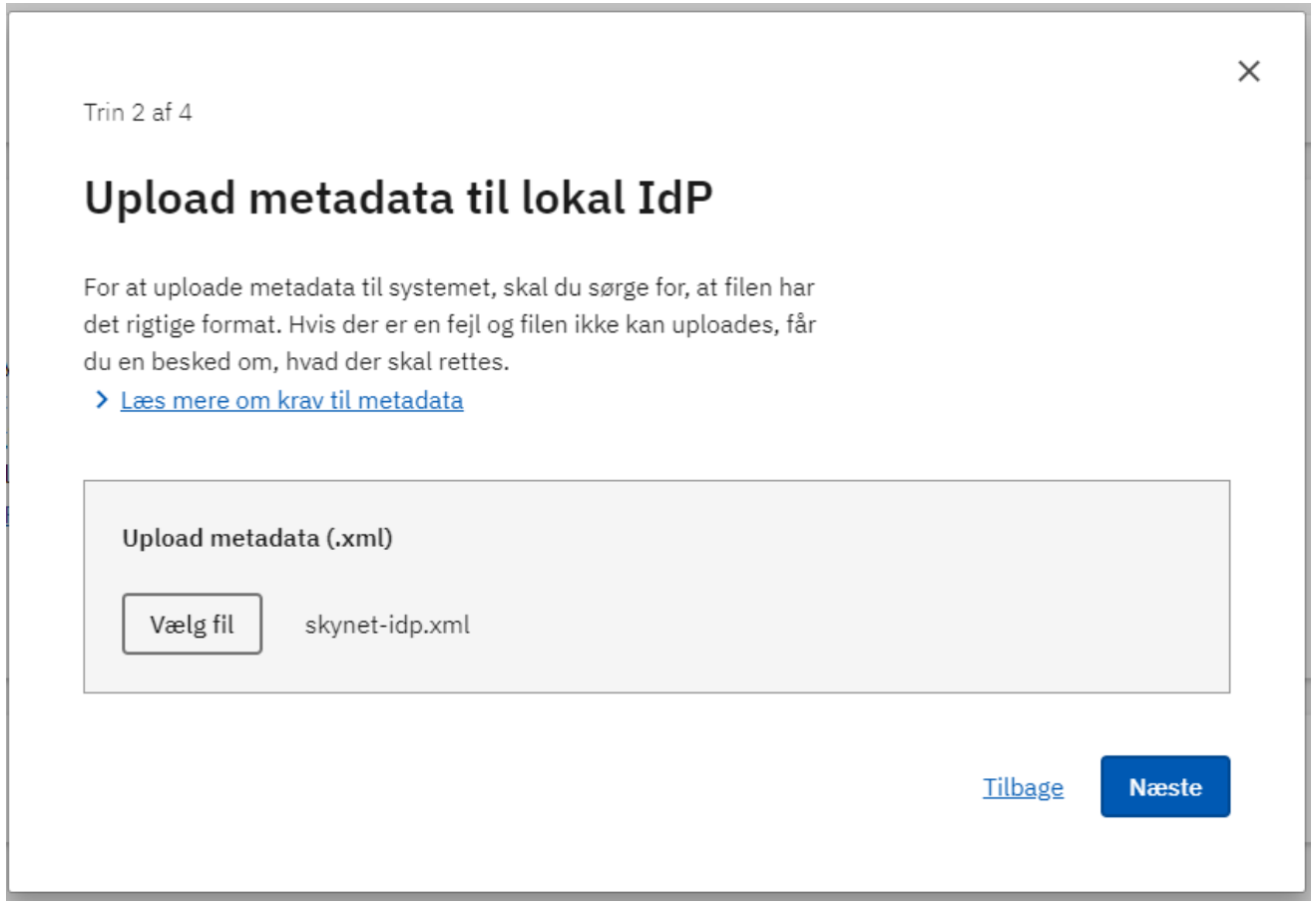
Erhverv



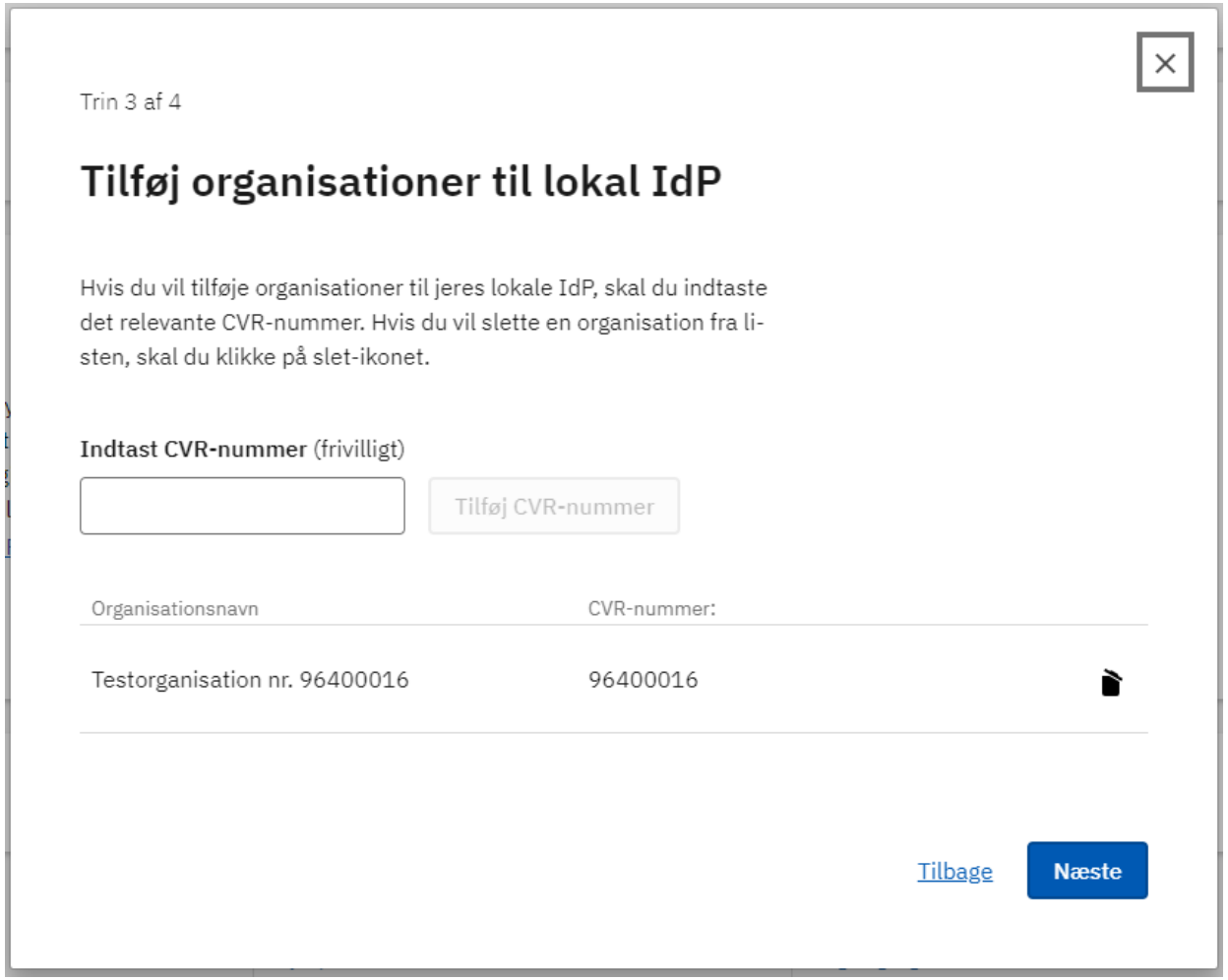


DIGITALISERINGSSTYRELSEN

Metadata med certifikat og entityid



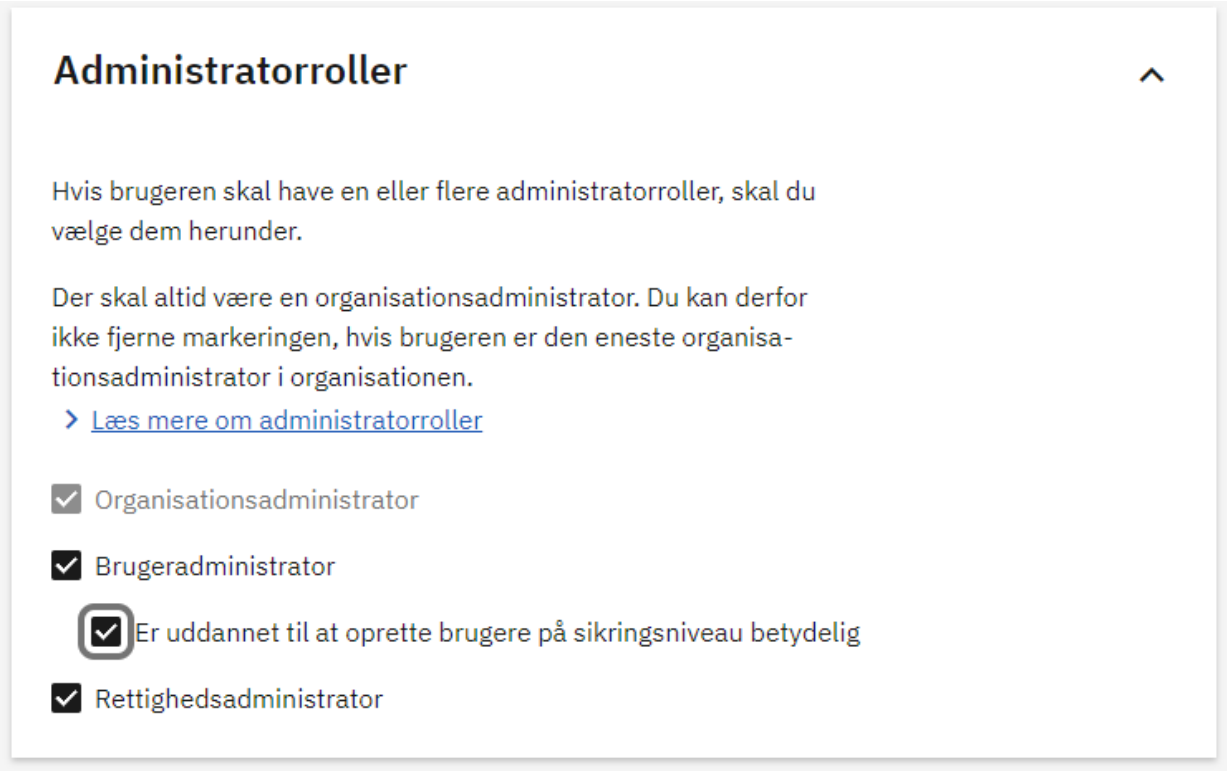
Tilføj evt. andre organisationer



Udpeg uddannet Brugeradministrator

Erhverv

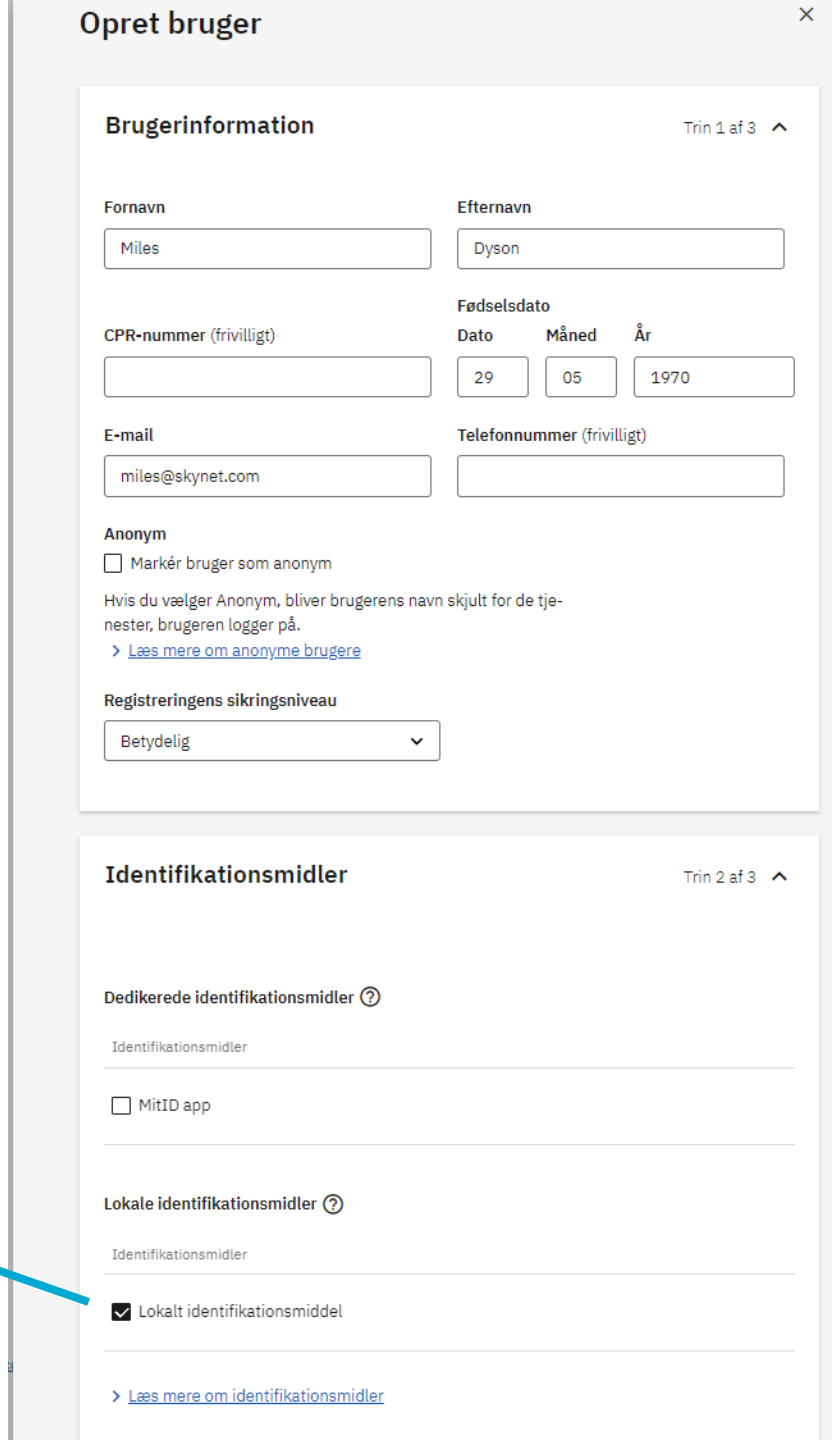
- Identiteter kan oprettes direkte aktive på NSIS Betydelig, men det kræver at brugeradministratoren er uddannet til at håndtere NSIS identitetssikring.



DIGITALISERINGSSTYRELSEN

Brugeradministrator: Opret bruger

- Brugeradministrator kan oprette direkte på sikringsniveau Betydelig.
  - Eller Lav, så benyttes normal identitetssikring via privat MitID.
- Brugernavn:
  - SubjectNameID fra IdP.



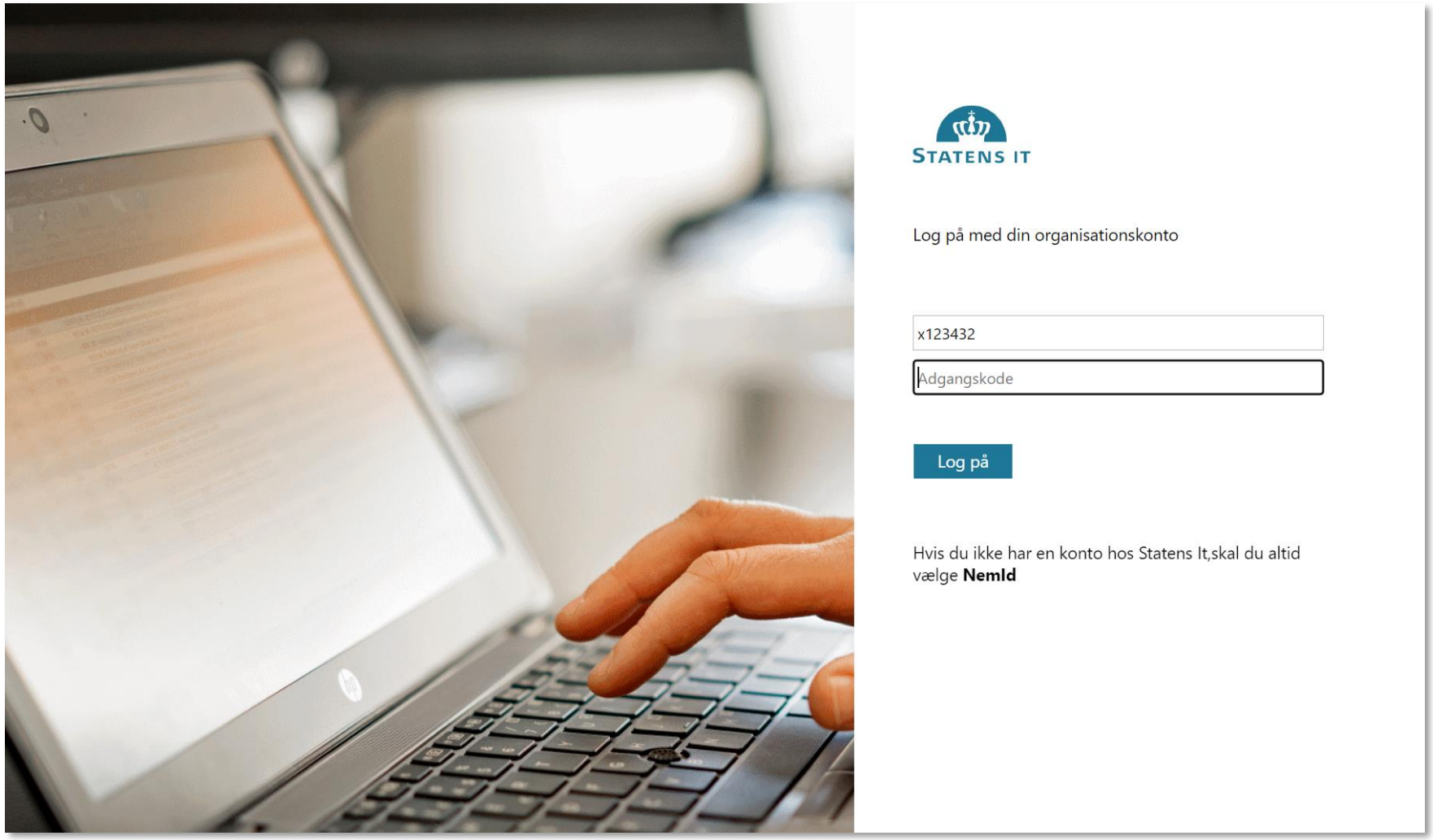
Bruger kan nu logge ind via IdPen

Erhverv

DIGITALISERINGSSTYRELSEN

Bruger sendes til den lokale IdP

Erhverv



DIGITALISERINGSSTYRELSEN

Opsamling: Hvad kan I gøre nu?

Hvad kan I gøre allerede nu?

Erhverv

Overvej, hvilke API'er der er relevante for jer

- Hvilke af de skitserede anvendelsesmuligheder passer til jeres behov og arbejdsgange?
- Overvej fordele og ulemper, herunder:
  - Gevinst ved automatisering af administration vs. manuel administration.
  - Omkostninger ved NSIS certificering, procedurer, udvikling og håndtering af identifikationsmidler.

Ønsker I IdM integration?

- Hent IdM API dokumentation.
- Testmiljø er tilgængeligt for alle.
- Hvis I ønsker at integrere med Lokal IdM NSIS-certificeret, anbefaler vi jer at påbegynde certificeringen snarest.

Ønsker I at etablere Lokal IdP?

- Påbegynd processen for etablering og implementering af Lokal IdP.
- Vi anbefaler jer at påbegynde NSIS anmeldelsen snarest.
- Testmiljø er tilgængeligt nu.

DIGITALISERINGSSTYRELSEN

Få hjælp og vejledning

Erhverv

Generelt om MitID Erhverv:

- Support og vejledninger: https://mitid-erhverv.dk/support/
- Om MitID Erhverv, priser, identifikationsmidler, administratorroller m.m.: https://mitid-erhverv.dk/info/

Integration med IdM:

- Læs mere om integration med IdM: https://mitid-erhverv.dk/avanceret/lokal-idm/
- Hent dokumentation og eksempel-kode for IdM API og Certifikat API: https://www.nemlog-in.dk/vejledningertiltestmiljo

Etablering af Lokal IdP:

- Læs mere om Lokal IdP: https://mitid-erhverv.dk/avanceret/lokal-idp/
- Hent OIOSAML Local Identity Provider Profile til brug mellem MitID Erhverv og en Lokal IdP: https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

DIGITALISERINGSSTYRELSEN

Spørgsmål

DIGITALISERINGSSTYRELSEN

Tak for i dag

Christian Schmidt-Madsen

It-arkitekt

Digitaliseringsstyrelsen

Tage Vestergård Madsen

It-arkitekt

Nets

Thomas Mostrup Nymand

Løsningsarkitekt

Nets

DIGITALISERINGSSTYRELSEN