DIGITALISERINGSSTYRELSEN

Erhverv

Bilag 7
Vilkår for anvendelse af Lokal IdP

Indholdsfortegnelse

Bilag

Bilag A Ledelseserklæring om anvendelse af Full-service Lokal IdP

Bilag B Krav til revisionserklæring for lokale registreringsprocesser

1 Indledning

Disse vilkår regulerer en Brugerorganisations anvendelse af en Lokal IdP med MitID Erhverv via NemLog-in's broker.

Ved at anvende en lokal IdP får en Brugerorganisation mulighed for lokalt at administrere og autentificere egne Erhvervsidentiteter og Identifikationsmidler, hvilket bl.a. giver mulighed for følgende:

- Erhvervsbrugere kan anvende de samme egen udstedte identifikationsmidler i såvel egen organisation som mod eksternt rettede Digitale Selvbetjeningsløsninger tilsluttet NemLog-in's Broker og øvrige brokere tilsluttet NemLog-in, der supporterer autentifikation med Lokal IdP.
- Brugerorganisationen kan opnå en enklere administration af Erhvervsbrugere, ved at disse kun administreres lokalt, og opdateringer synkroniseres med MitID Erhverv via API.

Tilknytning og konfiguration af en Lokal IdP til Brugerorganisationen skal ske ved Brugerorganisationens Organisationsadministrator.

Nærværende vilkår er i det hele underlagt vilkår for Brugerorganisationer. Såfremt der er modstrid, har vilkår for Brugerorganisationer forrang.

Alle de i vilkårene beskrevne Services er ikke nødvendigvis tilgængelige på tidspunktet for Brugerorganisationens accept af Vilkår. Brugerorganisationen skal særskilt orientere sig på mitid-erhverv.dk for nærmere beskrivelse af, hvilke Services der er tilgængelige samt evt. tidsplaner for introduktion af nye Services.

Bilagene til vilkårene udgør en integreret del heraf.

2 Kontaktinformation

Digitaliseringsstyrelsen har følgende kontaktinformation:

Digitaliseringsstyrelsen
Att. MitID-Erhverv Forvaltningen
Landgreven 4
1301 København K
E-mail: mitiderhverv@digst.dk

3 Definitioner

Definerede begreber følger definitioner fastlagt i vilkår for Brugerorganisationer.

4 NSIS-anmeldelse og overholdelse af NSIS-standarden

4.1 NSIS-anmeldelse og opretholdelse heraf

Forud for anvendelse af en Lokal IdP i MitID Erhverv skal den Lokale IdP NSIS-anmeldes som elektronisk identifikationsordning og identitetsbroker på mindst sikringsniveau Betydelig. NSIS-anmeldelsen er først gennemført, når den Lokale IdP er optaget på Digitaliseringsstyrelsens NSIS-positivliste. NSIS-anmeldelsen skal løbende opretholdes, jf. punkt 9 nedenfor.

4.2 Anvendelsesmodeller for Lokal IdP

En Lokal IdP kan anvendes efter to modeller: 1) Lokal IdP hos Brugerorganisationen og 2) Anvendelse via Full-service Lokal IdP hos tredjemand.

Ad. Model 1 Lokal IdP hos Brugerorganisationen

- Brugerorganisationen NSIS-anmelder egen Lokal IdP og er genstand for den revision, der er krævet efter NSIS standarden, herunder i forhold til tekniske forhold og processer. Brugerorganisationen kan lade en underleverandør udføre visse delopgaver, såfremt dette fremgår af NSIS anmeldelsen og revisionserklæringen.

  Model 1 omfatter også Lokal IdP'er, der er omfattet af en fælles NSIS-anmeldelse fra flere Brugerorganisationer, hvor alle Brugerorganisationer fremgår af samme anmeldelse og revisionserklæring.

  Efter model 1 fremgår Brugerorganisationen af NSIS-positivlisten uanset om Brugerorganisationen er NSIS-anmeldt alene eller omfattet af en fællesanmeldelse.

Ad. Model 2 Full-service Lokal IdP

- Brugerorganisationen benytter en Lokal IdP stillet til rådighed af en tredjemand. Tredjemand har anmeldt den Lokale IdP og varetager for Brugerorganisationen alle tekniske, sikkerhedsmæssige og processuelle forhold reguleret i NSIS herunder registrering og identitetssikring af brugere og udstedelse af identifikationsmidler, herunder særligt kravene i NSIS-standarden, afsnit 3.1.3. Den eksterne Full-service Lokal IdP er genstand for den revision, der er krævet efter NSIS-standarden. Efter model 2 er det tredjemand, der fremgår af NSIS positivlisten.

Brugerorganisationer, der ønsker at anvende en Full-service Lokal IdP efter model 2, er forpligtet til at underskrive den i Bilag A anførte ledelseserklæring og indsende denne til MitID-Erhverv Forvaltning, jf. punkt 2.

Ledelseserklæringen kan ligeledes downloades fra https://mitid-erhverv.dk/ledelseserklaering

Brugerorganisationen er i det hele ansvarlig for den anvendte Lokale IdP og for, at alle de i Vilkårene anførte krav er opfyldt uanset om en Lokal IdP anvendes efter model 1) eller model 2).

4.2.1 Særlige begrænsninger for Brugerorganisationer der anvender Full-service Lokal IdP

For at muliggøre den tekniske tilslutning af en Full-service Lokal IdP får brugerorganisationen tildelt en adgang, der svarer til den adgang, som en NSIS-anmeldt brugerorganisation tildeles.

En Brugerorganisation, der benytter en Full-service Lokal IdP i MitID Erhverv, jf. model 2 ovenfor, og ikke har NSIS-anmeldt en Lokal IdP, må alene acceptere invitationer fra en Full-service Lokal IdP, og må ikke tilslutte egen Lokal IdP til MitID Erhverv.

Det er således ikke tilladt for Brugerorganisationer, der ikke selv er NSIS-anmeldt, at straksoprette egne identiteter med et NSIS sikringsniveau, ligesom de ikke må oprette administratorer, der kan straksoprette identiteter[1]. Al aktivering af Brugerorganisationens brugere skal således ske via en NSIS-anmeldt løsning (enten MitID Erhverv eller en NSIS-anmeldt Lokal IdP).

[1] I MitID Erhverv brugerfladen er det tjekboksen 'Er uddannet til at oprette brugere på sikringsniveau betydelig', som ikke må afkrydses på Brugerorganisationens administratorer, når Brugerorganisationen ikke selv er NSIS-anmeldt.

5 Lokal IdP og MitID Erhverv

5.1 Oprettelse af Erhvervsidentiteter i MitID Erhverv

En forudsætning for, at en Erhvervsbruger kan autentificeres gennem en Lokal IdP tilsluttet MitID Erhverv er, at Erhvervsbrugeren er oprettet med tilknytning til Brugerorganisationen i MitID Erhverv, og at Erhvervsbrugeren i MitID Erhverv er registreret til at kunne anvende et lokalt identifikationsmiddel.

Brugerorganisationen kan oprette Identiteter i MitID Erhverv på følgende måder:

- Via brugergrænsefladen i MitID Erhverv
- Via IdM API snitfladen udstillet af MitID Erhverv

Oprettelse af erhvervsbrugere fra en Lokal IdP håndteres i relation til vederlag som en almindelig brugeroprettelse.

5.2 Tekniske krav til Lokal IdP

Tekniske krav til API integrationer mellem den Lokale IdP og MitID Erhverv samt relateret dokumentation fremgår af hjemmesiden for MitID Erhverv : https://www.mitid-erhverv.dk/avanceret/testorganisation-i-integrationstestmiljoet/

Integrationen mellem NemLog-in og den Lokale IdP skal overholde OIOSAML Local IdP Profile, som beskrevet på Digitaliseringsstyrelsens hjemmeside: https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

5.3 Vedligeholdelse af Erhvervsidentiteter

Brugerorganisationen er forpligtet til at sikre, at Erhvervsidentiteter altid er opdaterede i MitID Erhverv og synkroniserede med Brugerorganisationens egne registreringer af erhvervsbrugere, herunder at de slettes, når de ikke længere har behov for en Erhvervsidentitet. Dette gælder uanset hvilken metode til brugeroprettelse, der er anvendt, jf. punkt 5.1.

5.4 Udstedelse af certifikater og afgivelse af elektronisk signatur

5.4.1 Indledning

Erhvervsbrugere oprettet og identitetssikret via en Lokal IdP kan opnå mulighed for at afgive kvalificerede signaturer og kvalificerede segl via Den Danske Stats Signeringsløsning under anvendelse af identifikationsmidler fra den Lokal IdP enten ved 1) supplerende central identitetssikring og brugeraktivering af Erhvervsbrugere via MitID Erhverv, jf. punkt 5.4.2 eller 2) på baggrund af lokal identitetssikring og brugeraktivering hos den Lokale IdP, jf. punkt 5.4.3.

5.4.2 Central identitetssikring via MitID Erhverv

Erhvervsbrugere vil på baggrund af en supplerende identitetssikring med privat MitID i MitID Erhverv, få adgang til at afgive kvalificerede signaturer og kvalificerede segl via Den Danske Stats Signeringsløsning under anvendelse af identifikationsmidler fra en Lokal IdP

5.4.3 Lokal identitetssikring hos den Lokale IdP

Brugerorganisationen har på baggrund af lokal identitetssikring og brugeraktivering adgang til at afgive kvalificerede signaturer og kvalificerede segl via Den Danske Stats Signeringsløsning under anvendelse af identifikationsmidler fra en Lokal IdP efter en af følgende modeller:

a) Ved afgivelse af en revisionserklæring til Digitaliseringsstyrelsen om anvendte registreringsprocesser relateret til den lokale IdP, jf. punkt 5.4.3.1.

b) Ved afgivelse af en overensstemmelsesvurderingsrapport til Digitaliseringsstyrelsen, jf. nærmere i punkt 5.4.3.2

Efter begge modeller skal de lokale registreringsprocesser overholde kravene fastsat i artikel 24.1 i eIDAS forordningen (herefter eIDAS)[2].

Brugerorganisationens omkostninger relateret til lokal identitetssikring, herunder krav efter dette Bilag 7 er Digitaliseringsstyrelsen uvedkommende.

5.4.3.1 Afgivelse af en revisionserklæring

Brugerorganisationens lokale registreringsprocesser kan dokumenteres ved en revisionserklæring. De nærmere krav til revision fremgår af Bilag B. De interne processer kan enten være baseret på lokal verifikation af identitet med MitID eller kontrol af billedlegitimation.

5.4.3.2 Afgivelse af overensstemmelsesvurderingsrapport

Brugerorganisationens lokale registreringsprocesser kan dokumenteres i en overensstemmelsesvurderingsrapport, jf. eIDAS Artikel 20 udarbejdet af et overensstemmelsesvurderingsorgan, som bekræfter, at de lokale registreringsprocesser overholder kravene fastsat i eIDAS artikel 24.1.

Overensstemmelsesvurderingsrapporten skal stiles til Det Danske eIDAS tilsyn med kopi til Digitaliseringsstyrelsen. Det skal fremgå af rapporten, at vurderingen foretages med henblik på dokumentation af registreringsprocesser med det formål at kunne afgive kvalificerede signaturer og segl via MitID Erhverv.

Efter udløb af en overensstemmelsesvurderingsrapport, skal der indsendes en ny rapport senest 60 dage efter udløb.

5.4.3.3 Audit

Ved anvendelse af lokal Identitetssikring skal Brugerorganisationen med en rimelig frist og vederlagsfrit underlægge sig audit fra Digitaliseringsstyrelsen eller Digitaliseringsstyrelsens overensstemmelsesvurderingsorgan. Auditprocessen omfatter alene forhold vedrørende lokal Identitetssikring og adresserer således ikke Brugerorganisationens øvrige virksomhed eller aktiviteter. Brugerorganisationen er forpligtet til loyalt at medvirke til, og understøtte gennemførelse af audit. Dialog i relation til overensstemmelsesvurderingsorganet sker på engelsk og relevant dokumentation skal ligeledes fremlægges på engelsk.

6 Tilrådighedsstillelse af Full-service Lokal IdP

En Brugerorganisation, der er NSIS-anmeldt som elektronisk identifikationsordning og identitetsbroker, kan stille sin Lokale IdP til rådighed for andre brugerorganisationer og derved fungere som Full-service Lokal IdP i overensstemmelse med det i punkt 4 anførte. Brugerorganisationen, der fungerer som Full-service Lokal IdP, fastlægger selv sine aftaler med brugerorganisationer, der anvender Full-service Lokal IdP'en.

Digitaliseringsstyrelsen kan kræve afgivelse af særlige erklæringer i forbindelse med tilrådighedsstillelsen af en Full-service Lokal IdP.

[2] Europa-Parlamentets og Rådets forordning (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF

7 Identitetssikring af Erhvervsbrugere

Brugerorganisationen er ansvarlig for, at den anvendte Lokale IdP foretager korrekt identitetssikring af Brugerorganisationens Erhvervsbrugere.

Krav til identitetssikring og afledt sikringsniveau fremgår af NSIS-standarden.

Hvis Brugerorganisationen verificerer identiteten af den fysiske person på baggrund af MitID, vil det samlede sikringsniveau for erhvervsbrugeren maksimalt svare til NSIS sikringsniveauet for det pågældende MitID.

8 Brugerorganisationens ansvar

Brugerorganisationens generelle ansvar er reguleret i Vilkår for Brugerorganisationer.

Brugerorganisationens erstatningsansvar relateret til håndtering af lokale identiteter, identifikationsmidler og autentifikationer følger NSIS-standarden, herunder de krav som følger af NSIS afsnit 7.3 (Ansvar og forsikring).

Ovenstående ansvar er uafhængigt af om Brugerorganisationen anvender en Lokal IdP efter model 1 eller model 2.

9 Løbende opretholdelse af NSIS-anmeldelse og revision

Den i punkt 4 anførte NSIS-anmeldelse skal løbende opretholdes for den anvendte Lokale IdP, og krav i NSIS-standarden skal løbende overholdes, herunder i forhold til revision.

Hvis NSIS-anmeldelsen for den anvendte Lokale IdP – uanset årsag hertil - ikke kan opretholdes, skal Brugerorganisationen straks ophøre med anvendelse heraf og afregistrere den Lokale IdP i MitID Erhverv.

Digitaliseringsstyrelsen er berettiget til at lukke for adgangen til den Lokale IdP, såfremt den ikke længere fremgår af NSIS positivlisten.

10 Løbende opretholdelse af grundlag for udstedelse af certifikater og afgivelse af signaturer

Den i punkt 5.4.3 anførte revisionserklæring eller overensstemmelsesvurdering skal løbende opretholdes for den anvendte Lokale IdP, hvis retten til at udstede kvalificerede signaturer og segl skal bibeholdes.

Digitaliseringsstyrelsen kan (og vil i henhold til eIDAS være forpligtet til) uden varsel lukke for adgang til at afgive kvalificerede signaturer og kvalificerede segl via Den Danske Stats Signeringsløsning, såfremt Brugerorganisationen ikke rettidigt leverer den i punkt 5.4.3.1 anførte revisionserklæring eller den i punkt 5.4.3.2 anførte overensstemmelsesvurderingsrapport.

Tilsvarende kan Digitaliseringsstyrelsen uden varsel lukke for adgangen til at afgive kvalificerede signaturer og segl fra via Den Danske Stats Signeringsløsning, hvis revision eller overensstemmelsesvurdering påviser væsentlige fejl, eller hvis sådanne fejl konstateres på baggrund af et audit. Digitaliseringsstyrelsen er ligeledes berettiget til at lukke for adgangen til at afgive kvalificerede signaturer og segl, hvis den Lokale IdP ikke loyalt medvirker til audit.

11 Meddelelse om ophør eller afregistrering

Brugerorganisationen er ved ophør eller afregistrering af en Lokal IdP forpligtet til at meddele MitID Erhverv Forvaltningen om årsagen hertil. Brugerorganisationen er ligeledes forpligtet til at aflevere en afsluttende revisionserklæring for den periode, der endnu ikke er revideret.

Bilag A Ledelseserklæring om anvendelse af Full-service Lokal IdP

Ledelseserklæring om anvendelse af Full-service Lokal IdP

CVR-nr*:	[Indsæt brugerorganisationens CVR-nummer]
Brugerorganisation	[Indsæt navn på brugerorganisationen]
Navn*:	[Indsæt navn på ledelsesrepræsentant]
E-mailadresse:	[Indsæt e-mailadresse på ledelsesrepræsentant]

Lokal IdP	[Indsæt navn på Full-service Lokal IdP]
CVR-nummer:	[Indsæt CVR-nummer på Leverandøren af Lokal IdP]

På tro og love erklærer undertegnede ledelsesrepræsentant for Brugerorganisationen følgende:

- At undertegnede varetager en rolle som ledelsesrepræsentant for Brugerorganisationen og kan forpligte denne i forhold til denne ledelseserklæring og de tilhørende vilkår for tilslutning af Lokal IdP
- Brugerorganisationen ønsker at tilknytte ovenstående Lokal IdP til Brugerorganisationen efter modellen Full-service Lokal IdP med henblik på, at Brugerorganisationen kan anvende denne til autentifikation af lokale brugere i sammenhæng med MitID Erhverv.
- Ved identitetssikring af brugere og udstedelse af identifikationsmidler baserer Brugerorganisationen sig udelukkende på den service og de processer, der er udføres af den valgte Full-service Lokale IdP, og som er indeholdt i revisionen heraf, og som danner grundlaget for NSIS-anmeldelsen for den Lokale IdP.
- Brugerorganisationen varetager ikke opgaver eller udfører aktiviteter reguleret af NSIS i tilknytning til den anvendte Full-service Lokale IdP, herunder registrering eller identitetssikring af brugere.
- Det sikres, at eventuelle øvrige lokale IdP'er Brugerorganisationen opretter enten er dækket af en selvstændig ledelseserklæring om anvendelse af Full-service Lokal IdP eller er tilknyttet Brugerorganisationen selv, og er NSIS-anmeldt.
- Denne ledelseserklæring anvendes alene som grundlag for tilslutning af ovenstående Lokale IdP. Såfremt Brugerorganisationen ønsker at anvende øvrige Full-service Lokale IdP'er tilsluttet MitID Erhverv, sikrer Brugerorganisationen, at der afgives en separat ledelseserklæring herom.
- Brugerorganisationen er i det hele ansvarlig for de services, der udføres af den Lokale IdP og påtager sig et ansvar svarende hertil over for Digitaliseringsstyrelsen og øvrige parter.
- På Brugerorganisationens vegne indestår jeg for, at ovenstående oplysninger er korrekte, og at jeg i øvrigt er bekendt med vilkår for Lokal IdP udarbejdet af Digitaliseringsstyrelsen.

Dato: […]

Underskrift: […]

Bilag B Krav til revisionserklæring for lokale registreringsprocesser

Revisionserklæringen skal dække nedenstående kontrolmål:

Kontrolmål 1)

Der er implementeret en effektiv registreringsproces for erhvervsbrugere, der skal kunne signere med kvalificerede signaturer eller segl fra Den Danske Stat Tillidstjenester via organisationens Lokale IdP, som sikrer, at mindst én af flg. betingelser er opfyldt:

a) Den lokale registreringsproces for erhvervsbrugere anvender privat MitID til verifikation af den **fysiske person** via login på mindst NSIS sikringsniveau Betydelig, *eller*:

b) Erhvervsbrugere registreres på baggrund af fysisk fremmøde med tilhørende kontrol af nationalt anerkendt billedlegitimation enten i form af pas eller kørekort. Typen af legitimation, udstedelsesland samt løbenummer (pas- eller kørekortnummer) registreres. Kontrollen omfatter som minimum flg. punkter:

   a. Legitimationen ikke er udløbet.
   b. Legitimationen indeholder fornavn, efternavn og CPR-nummer, som modsvarer en person registreret i organisationens autoritative personale- eller HR-register.
   c. Personen kan svare på kontrolspørgsmål ift. HR-registreringen om f.eks. titel, nærmeste leder, ansættelsessted, ansættelsestidspunkt mv.
   d. Billedet på legitimationen ligner med høj grad af sikkerhed brugeren.
   e. Legitimationen fremstår ikke beskadiget eller som forsøgt ændret eller forfalsket.
   f. Ved brug af dansk digitalt kørekort verificeres dette digitalt ved scanning af QR-kode med kontrollantens egen kørekort app. Slutbrugeren skal åbne sin app, vælge 'Kontrol' og vælge ID, så QR-koden vises. Kontrollanten scanner herefter QR-koden med egen kørekort app. Her skal der fremgå et grønt checkmark og ordet 'Gyldig' i bunden af skærmen. Det overførte navn og CPR-nummer skal matche brugerens øvrige dokumenterede oplysninger.

Registreringsprocessen skal være dækket af organisationens NSIS-anmeldelse og dermed efterleve kravene i standarden.

Kontrolmål 2)

Organisationen har implementeret effektive kontroller som sikrer, at det alene er erhvervsbrugere, der er registreret med ovennævnte proces, der af organisationen er tildelt adgang i MitID Erhverv til at kunne signere med kvalificeret signatur.

Formålet med ovenstående kontrolmål er at understøtte, at organisationer kan have forskellige registreringsprocesser med forskellig styrke til forskellige medarbejdergrupper. Der er alene krav om, at de medarbejdere, der oprettes med adgang til kvalificeret signering i MitID Erhverv, skal være underlagt kravene under kontrolmål 1), og der er således ikke i noget til hinder for, at brugere, der ikke oprettes med adgang til kvalificeret signering i MitID Erhverv, håndteres med andre processer. Det er Brugerorganisationens ansvar at have fornødne processer og kontrolmekanismer til rådighed for at kunne adskille sådanne brugere.

Erklæringsperiode og -type

Erklæringen skal afgives på engelsk som en ISAE 3000 erklæring med høj grad af sikkerhed.

Første erklæring afgives som en type 1 erklæring (for en specifik dato) mens efterfølgende erklæringer afgives kontinuerligt (fx årligt) som en type 2 erklæring for en periode på mindst 6 måneder, så perioden fra seneste erklæringsdato dækkes kontinuerligt.