DIGITALISERINGSSTYRELSEN

Guide til implementering af lokal IdP og tilslutning til MitID Erhverv

Version 1.2

Version	Dato	Bemærkninger
1.0	20/12-2019	Første version klar til publicering.
1.1	04/02-2021	Tidslinje tilrettet og terminologiske opdateringer ("MitID Erhverv"), og mindre sproglige præciseringer foretaget. Præciseret at tilslutning af lokal IdM og IdP sker gennem erhvervsløsningen og ikke administrationsportalen.
1.2	28/10-2022	Tilrettet tidslinje, terminologi vedr. MitID Erhverv og referencer til testmiljøer.

DIGITALISERINGSSTYRELSEN

Indholdsfortegnelse

1. Indledning og formål

Denne guide beskriver en række aspekter vedr. lokale IdP'er og deres interaktion med NemLog-in3 og MitID Erhverv[1].

Formålet er gøre det enklere at implementere og tilslutte en lokal IdP ved at skabe et samlet overblik over de forskellige opgaver af både teknisk og organisatorisk karakter, der er involveret i processen.

Fremstillingen er på et overordnet niveau, idet NemLog-in3 løsningen ikke er færdigudviklet endnu. Det er dog fra oktober 2022 muligt at tilgå tidlige udgaver af funktionalitet til lokal IdP og IdM API i NemLog-in's beta-testmiljø.

Det anbefales at komme tidligt i gang med analyseopgaven samt forberedelsen af implementeringen af lokale IdP'er, idet dette for mange organisationer vil udgøre en ikke ubetydelig opgave.

2. Hvad er en brugerorganisation med lokal IdP?

En brugerorganisation er en organisation (virksomhed, myndighed, frivillig forening osv.), hvis erhvervsbrugere skal logge sikkert på on-line tjenester i arbejdsmæssigt regi. I denne henseende er betegnelsen *brugerorganisation* altså en organisation, som tilsluttes MitID Erhverv (NemLog-in's erhvervsløsning), der erstatter NemID til erhverv. MitID Erhverv løsningen rummer to forskellige modeller (som evt. kan kombineres):

a) Brugerorganisationen kan bruge de nye erhvervsidentiteter i MitID Erhverv i samspil med MitID identifikationsmidler (central model). Denne løsning er en færdig 'pakke' som brandes 'MitID Erhverv', og er den mulighed, som mest ligner den nuværende erhvervsløsning i NemID (dog med en række forskelle).

b) Brugerorganisationer får desuden mulighed for selv at stå for at håndtere deres erhvervsidentiteter decentralt – via en såkaldt lokal IdP (Identity Provider – på dansk 'identitetsgarant') ofte kombineret med et lokalt IdM (Identity Management) system, som kan tilsluttes NemLogin. Muligheden for at håndtere erhvervsidentiteter decentralt omfatter processer vedr. identitetssikring af egne erhvervsbrugere, udstedelse af identifikationsmidler til egne erhvervsbrugere, og autentifikation af egne erhvervsbrugere inkl. videreformidling af deres identitet og det aktuelle sikringsniveau for autentifikationen til en tjenesteudbyder (eller anden broker som NemLog-in, som igen videreformidler til tjenesteudbydere). I termer af NSIS-standarden agerer en lokal IdP således både i rollen som NSIS Identitetsbroker og Elektronisk Identifikationsordning.

[1] https://mitid-erhverv.dk

Dette notat koncentrer sig alene om mulighed b) ovenfor.

Det lokale log-in (fra en Lokal IdP) kan via NemLog-in (i rollen som broker) sendes videre (omveksles) til de tjenester, som er tilsluttet NemLog-in - via princippet om føderation af identiteter. Derfor vil et lokalt login kunne anvendes mod alle offentlige tjenesteudbydere samt de private tjenesteudbydere, der tilslutter sig NemLog-in som illustreret på nedenstående figur:

Grundlaget for tillid i føderationen er NSIS (National Standard for Identiteters Sikringsniveauer), som stiller krav dels til identitetsbrokere og dels til udstedere af elektroniske identifikationsmidler.

2.1 Fordele ved en lokal IdP

Ved at implementere en lokal IdP får en brugerorganisation frihed til at håndtere egne erhvervsidentiteter og identifikationsmidler, hvilket kan give en række fordele:

- Erhvervsbrugere kan anvende de samme identifikationsmidler i såvel egen organisation som mod eksternt rettede tjenester – fx samme brugernavn, password, app, fysisk enhed osv.
- Lokale identifikationsmidler kan fx integreres med fysiske adgangskort til egen organisation, således at erhvervsbrugere oplever en enklere og mere sammenhængende adgang i deres dagligdag.
- Brugerorganisationen kan opnå en enklere administration af sine erhvervsbrugere ved at brugerne kun administreres lokalt, og opdateringer synkroniseres med MitID Erhverv via IdM API.

Disse fordele skal naturligvis opvejes mod det arbejde og de omkostninger og ansvar, der er forbundet med at etablere og drive en lokal IdP – herunder omkostning til sikkerhed, drift og årlige revisionserklæringer. Det er derfor en overvejelse værd for en brugerorganisation, om der er tilstrækkelig modenhed i organisationen i forhold til processer og sikkerhed til at kunne løfte opgaven som lokal IdP, eller om organisationen er bedre tjent med at anvende MitID Erhverv baseret på MitID identifikationsmidler.

2.2 Typer af brugerorganisationer

I denne guide fokuseres på brugerorganisationer, som ønsker at udstede egne (lokale) identifikationsmidler til erhvervsbrugere. Gennem den lokale IdP (som autentifikationsservice) får disse erhvervsbrugere mulighed for at logge på tjenesteudbydere tilsluttet via NemLog-in. Brugerorganisationen kan naturligvis også forbinde IdP'en til andre brokere eller domæner.

Det er endvidere et krav, at alle erhvervsidentiteter skal være oprettet centralt i MitID Erhverv, før de kan blive autentificeret via en lokal IdP og fødereret gennem NemLog-in's broker. Dette kan enten ske ved, at en administrator for brugerorganisationen tilgår MitID Erhverv's brugerflader til administration, eller at brugerorganisationen anvender sit eget IdM-system, der synkroniserer erhvervsidentiteterne via

NemLog-in's IdM API til dette. Det er i princippet muligt at administrere medarbejderidentiteterne lokalt og synkronisere dem til NemLog-in via et IdM-system uden at have en lokal IdP, hvis man vil anvende MitID identifikationsmidler.

Sammenhængene er illustreret i nedenstående tabel:

Systemer hos brugerorganisation	Eksempel på anvendelse
Hverken IdP eller IdM	Brugerorganisation som alene anvender MitID identifikationsmidler for deres erhvervsidentiteter og vedligeholder disse i den centrale MitID Erhverv brugergrænseflade.
Kun lokal IdP	Brugerorganisation som udsteder egne identifikationsmidler, men vedligeholder erhvervsidentiteter centralt i MitID Erhverv via dennes brugergrænseflade.
Kun lokal IdM	Brugerorganisation som alene anvender MitID identifikationsmidler i MitID Erhverv, men som gerne vil vedligeholde brugerne i et lokalt system og synkronisere disse via IdM API til NemLog-in.
Både lokal IdP og lokal IdM	Brugerorganisation som både udsteder lokale identifikationsmidler og ønsker at vedligeholde brugerne lokalt i eget system, hvorfra de synkroniseres via IdM API til MitID Erhverv.

2.3 Hovedopgaver for en lokal IdP

Der er to hovedopgaver for en lokal IdP, der ønsker opkobling til NemLog-in:

a) Implementering af NSIS-standarden på det sikringsniveau, der ønskes anmeldelse på. Herved kan der udstedes identifikationsmidler til erhvervsbrugere og fødereres med NemLog-in's broker. Implementeringen afsluttes med en anmeldelse, der omfatter nødvendige revisionserklæringer.

b) Integration med NemLog-in's snitflade til den lokale IdP via OIOSAML 3 protokollen.

Disse to opgaver beskrives nærmere nedenfor i den resterende del af dokumentet.

3. Implementering af NSIS-standarden

Brugerorganisationer med lokal IdP vil optræde som identitetsgarant for erhvervsidentiteter udstedt til egne erhvervsbrugere, og via NemLog-in kan et lokalt log-in give adgang til alle tjenesteudbydere tilsluttet NemLog-in herunder alle offentlige tjenester. Den lokale IdP bliver dermed en vigtig brik i sikkerheden for det samlede økosystem. Grundlaget for tillid til identiteterne etableres gennem overholdelse af fælles krav og spilleregler defineret i National Standard for Identiteters Sikringsniveauer (NSIS). Det er således en forudsætning for tilslutning af en lokal IdP til den fællesoffentlige infrastruktur, at den lever op til kravene i standarden.

NSIS definerer en proces for anmeldelse, hvor lokale løsninger (fx lokal IdP) skal dokumentere overholdelse af kravene ved at indsende teknisk dokumentation, en ledelseserklæring og på niveau Betydelig og Høj også en revisionserklæring, hvor en statsautoriseret revisor erklærer at have efterset, at kravene er opfyldt.

Lever den lokale IdP ikke op til kravene i NSIS på et givet sikringsniveau, vil den ikke kunne betjene de tjenesteudbydere, som kræver dette sikringsniveau. Her kan brugerorganisationen i stedet benytte centrale erhvervsidentiteter udstedt i MitID Erhverv (baseret på MitID identifikationsmidler) til tjenester, der kræver dette (eller højere niveauer).

Endelig skal det bemærkes, at de personer der her omtales som 'erhvervsbrugere' ikke behøver være ansat i brugerorganisationen. En brugerorganisation kan ligeledes udstede erhvervsidentiteter til personer, der alene er associeret med brugerorganisationen, hvilket fx kan inkludere revisor eller advokat, der som eksterne aktører arbejder for brugerorganisationen.

3.1 Primære opgaver i NSIS-implementering

Implementering af NSIS-standarden hos en brugerorganisation involverer en række forskellige discipliner – både tekniske, organisatoriske og sikkerhedsmæssige. Det er derfor vigtigt ikke at betragte opgaven som et rent teknisk implementeringsprojekt.

Der er typisk tre hovedprocesser, der skal etableres og systemunderstøttes:

a) Proces for identitetssikring af erhvervsbrugere.

b) Proces for udstedelse af identifikationsmidler til erhvervsbrugere.

c) Etablering og udstilling af autentifikationstjeneste, som kan autentificere erhvervsbrugere via de udstedte identifikationsmidler (selve IdP'en).

De to første uddybes nedenfor mens den tredje beskrives i næste kapitel.

Figur 1 Proces for udstedelse af lokale identifikationsmidler

Ud over design af processer og systemer, er der en række øvrige forhold, som også skal tages i betragtning i en implementering af NSIS:

- Der skal formentlig ske uddannelse af administratorer eller andet personale, som udfører kontroller fx vedr. identitetssikring, samt gennemføres øvrig organisatorisk implementering.
- Der skal etableres revisionsspor, så processerne kan auditeres af en revisor.
- Der skal etableres et ledelsessystem til styring af sikkerhed og risici (ISMS – Information Security Management System), som dækker kontrollerne i NSIS.
- Der skal som tidligere nævnt gennemføres revision af ekstern revisor. Dette beskrives yderligere i afsnit 3.3.

Det anbefales, at brugerorganisationer, der ønsker at etablere en lokal IdP, orienterer sig mod NSIS-sikkerhedskrav og revisionsvejledning [NSIS]. Det anbefales endvidere at tage tidlig dialog med revisor i forhold til at sikre en tilstrækkelig dokumentation og sporbarhed for overholdelse af såvel tekniske som organisatoriske krav.

3.1.1 Identitetssikring af erhvervsbrugere

I denne proces skal identiteten af erhvervsbrugere verificeres, hvilket involverer to dele:

- Verifikation af identiteten af den fysiske person.
- Koblingen mellem den fysiske person og brugerorganisationen (en erhvervsidentitet i NSIS opfattes som en kobling mellem fysisk person og en juridisk enhed).

Brugerorganisationen skal indledningsvis gøre sig klart, hvilket sikringsniveau, den lokale IdP skal rettes imod. Det afhænger helt af kravene fra de tjenester, erhvervsbrugere skal tilgå, herunder følsomheden af de data, som tilgås. Hvis erhvervsbrugernes behov er differentierede, kan det være en overvejelse at lade en lokal IdP håndtere erhvervsbrugere og tjenester på niveau Betydelig, mens erhvervsbrugere med behov for autentifikation på niveau Høj benytter den centrale løsning (erhvervsidentiteter i NemLog-in baseret på MitID identifikationsmidler). Herved behøver den lokale IdP ikke selv opfylde kravene på niveau Høj. Alternativet er, at den lokale IdP anmeldes på sikringsniveau Høj – således at den kan håndtere erhvervsbrugere med dette behov med en rent lokal løsning.

Til at verificere identiteten af den bagvedliggende fysiske person kan man enten etablere en organisatorisk funktion eller enhed, der kontrollerer identitetsdokumenter som fx pas eller kørekort, eller man kan basere identitetssikring på autentifikation med brugerens private NemID eller MitID (fx i en self-service indrulleringsapplikation). Sikringsniveauet for en erhvervsidentitet vil her aldrig kunne blive højere end sikringsniveauet for det private NemID eller MitID, der indrulleres på baggrund af. Typisk vil et MitID og NemID være på niveau Betydelig, og hvis der sigtes mod niveau Høj for erhvervsidentiteter og identitetssikring via autentifikation med privat identifikationsmiddel, kan de pågældende erhvervsbrugere møde op i borgerservice for at få udstedt et MitID på niveau Høj, som herefter kan bruges til indrullering af en erhvervsidentitet på niveau Høj.

Til at sikre koblingen mellem den fysiske person og brugerorganisationen, vil brugerorganisationen ofte udpege en eller flere betroede administratorer, som er bemyndiget til at registrere, om en given fysisk

person har en erhvervsrelation til organisationen (fx på baggrund af autoritative data i et HR-system), eller på anden vis er associeret med organisationen (bestyrelsesmedlem, revisor, o.lign.).

Endelig vil erhvervsidentiteten, efter identitetssikring er gennemført, typisk blive registreret i et lokalt system (fx IdM system, et directory som Microsoft Active Directory eller lignende). Det er dog også obligatorisk at oprette identiteten i NemLog-in's centrale erhvervsløsning. Dette kan enten ske via en brugergrænseflade i NemLog-in, som tilgås af en administrator fra brugerorganisationen, eller det kan ske via et API, som anvendes af det lokale IdM system til at provisionere den nye erhvervsidentitet. Sidstnævnte kræver tilslutning af IdM-systemet til NemLog-in.

3.1.2 Aktivering af erhvervsbrugere

Normalt skal en erhvervsbruger oprettet af en brugerorganisation aktiveres i MitID Erhverv, før identiteten kan anvendes. Hvis erhvervsidentiteter ønskes oprettet via MitID Erhvervs brugergrænseflade, vil aktiveringen normalt ske ved at brugeren får tilsendt et aktiveringslink fra MitID Erhverv med instruktion om at autentificere sig med privat identifikationsmiddel.

Når en brugerorganisation med lokal IdP er NSIS anmeldt (som udsteder af identifikationsmidler), kan den få lov til selv stå for identitetssikringen af den fysiske person knyttet til erhvervsidentiteter. I dette tilfælde kan brugerorganisationen ***straksaktivere*** erhvervsidentiteten i forbindelse med oprettelsen, hvorved der ikke er behov for yderligere skridt, før identiteten kan anvendes.

3.1.3 Udstedelse af identifikationsmidler

Efter identitetssikring af erhvervsbrugeren er gennemført, skal brugerorganisationen udstede et identifikationsmiddel, og dette skal udleveres sikkert til erhvervsbrugeren. Typisk vil dette være en kombination af et brugernavn+kodeord samt en fysisk enhed (fx App på mobilenhed, smart card, U2F-token etc.), der kan anvendes til to-faktorautentifikation, hvilket er et krav i NSIS standarden for at kunne nå niveau Betydelig.

Det er vigtigt på forhånd at sikre sig, at de planlagte identifikationsmidler opfylder de tekniske krav, som stilles på de forskellige sikringsniveauer[2], samt at de teknisk kan fungere i de lokale systemer, som skal understøttes. Dette kræver således en analyse af brugerorganisationens infrastruktur og erhvervsbrugernes brugsmønster. Der kan fx være forskel på, hvilke identifikationsmidler der er velegnede til kontorarbejde og til arbejde på farten (fx personale i hjemmeplejen). Ligeledes kan det spille en rolle, hvilket udstyr erhvervsbrugerne allerede har til rådighed, herunder om de fx har fået udleveret personlige smartphones fra organisationen, eller om de anvender delt udstyr.

3.2 Øvrige områder i NSIS vedr. håndtering af identifikationsmidler

Der er en række øvrige områder i NSIS, der stiller krav til håndtering af identifikationsmidler. Det er derfor vigtigt at tage højde for disse, så alle aspekter er dækket. Dette gælder eksempelvis processer vedr. spærring, genaktivering, suspendering mv.

[2] Der er særlige krav til identifikationsmidler på niveau Høj – fx må de enkelte faktorer ikke være kopierbare.

3.3 Revisionserklæringer

Et vigtigt grundlag for tilliden i NSIS er den dokumentation, der skal leveres for opfyldelse af kravene på de forskellige sikringsniveauer. For at sikre en høj grad af troværdighed indgår revisionserklæringer fra en uafhængig, statsautoriseret revisor (valgt af den brugerorganisation, som vil anmelde sin løsning).

Revisionen for en lokal IdP omfatter som tidligere nævnt både efterlevelsen af NSIS-krav vedr. håndtering af elektroniske identifikationsmidler og som identitetsbroker (dvs. kravene i kapitel 3, 4, 5 og 6 i NSIS fraregnet evt. afsnit 3.1.3, hvis juridiske personer ikke håndteres). Her skal der på niveau Betydelig og Høj leveres en ISAE 3000 erklæring i henhold til den revisionsvejledning, der er udarbejdet til NSIS, som beskrevet i NSIS 4.1.7.

Der må påregnes et vist arbejde med at indhente de krævede revisionserklæringer herunder at sikre, at den relevante dokumentation for systemer og processer er fyldestgørende samt tilgængelige for revisor.

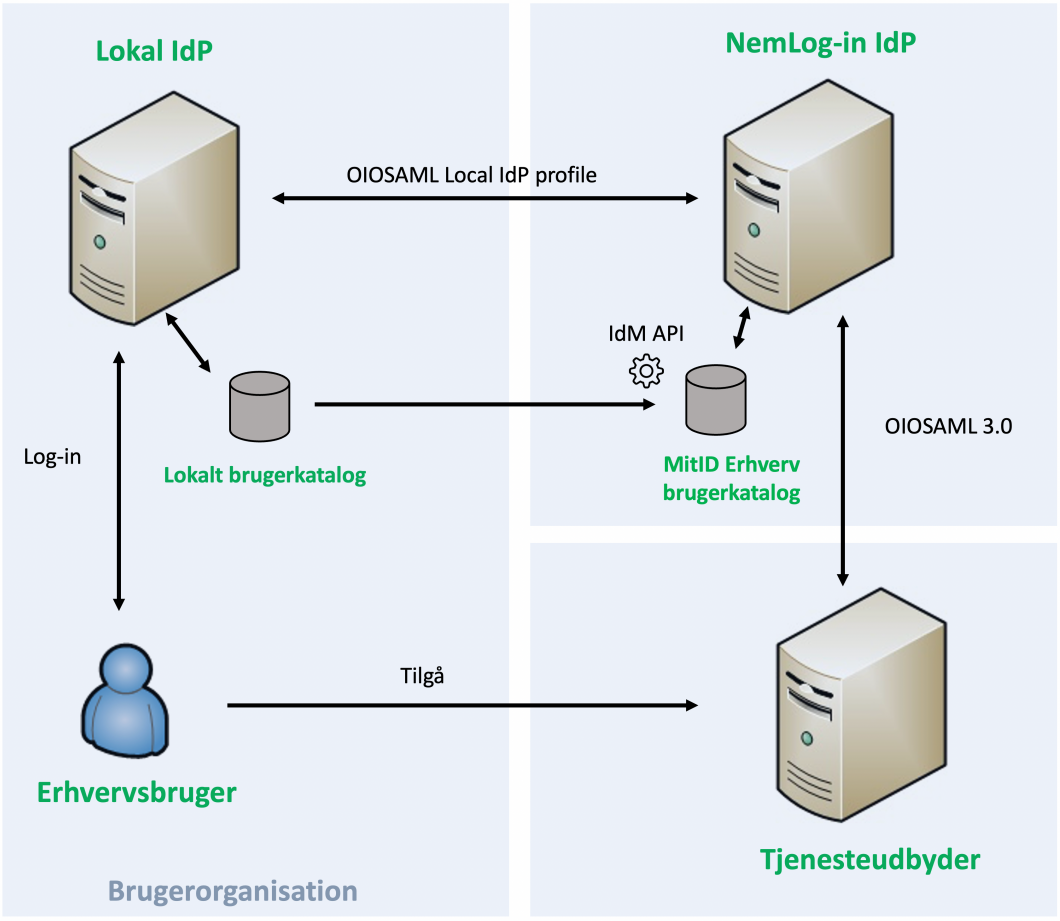
4. Integration med NemLog-in via OIOSAML 3.0

4.1 Snitflade til autentifikation

Den væsentligste snitflade mellem en brugerorganisation med en lokal IdP og NemLog-in relaterer sig til brugerautentifikation, hvor NemLog-in vil anmode den lokale IdP om at autentificere en lokal erhvervsbruger. Denne kommunikation sker via OIOSAML 3.0 profilen for lokale IdP'er, og specifikationen kan hentes fra Digst.dk (se afs. 7 Referencer).

Den lokale IdP profil rummer større fleksibilitet i forhold til den almindelige OIOSAML 3.0 profil, som tjenesteudbydere integrerer til NemLog-in med. Den lokale IdP profil er dermed lettere at understøtte med standardprodukter, der kan have en del begrænsninger i understøttelse af SAML protokollen.

Det frarådes at forsøge at udvikle en SAML-implementering fra bunden, og man bør i stedet basere implementeringen på et standardprodukt eller referenceimplementering, som i forvejen har understøttelse for SAML standarden og blot skal konfigureres. For en omfattende liste af både kommercielle- og open source produkter kan henvises til siden: https://en.wikipedia.org/wiki/SAML-based_products_and_services



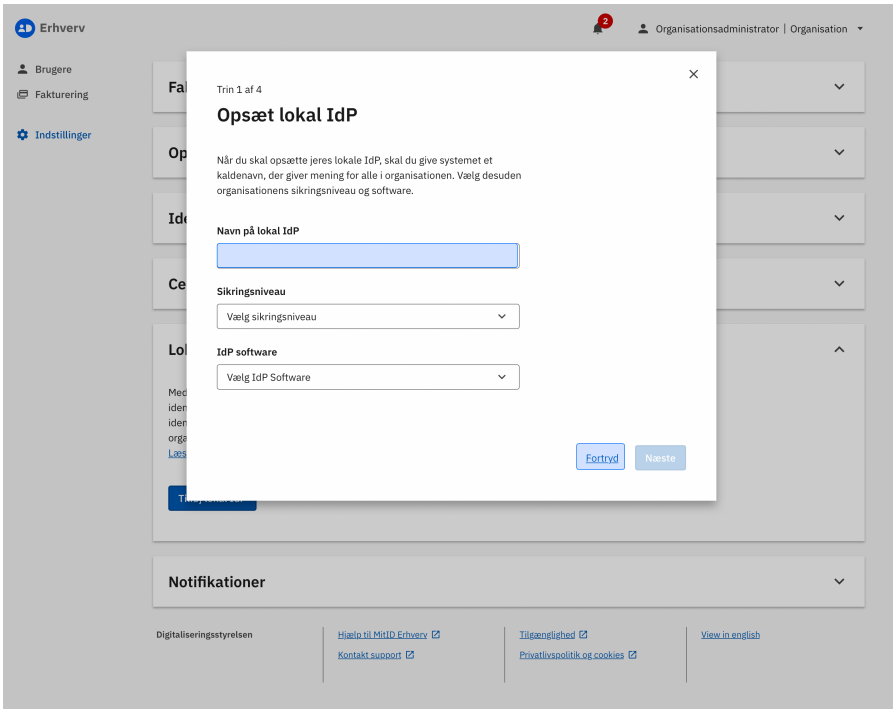
Figur 2- Samspil mellem Lokal IdP og NemLog-in IdP

Bemærk at figuren ovenfor er simplificeret med henblik på at formidle et samlet overblik. Kommunikationen mellem lokal IdP og NemLog-in IdP sker eksempelvis typisk via brugerens browser.

4.2 Tilslutning af lokal IdP til NemLog-in

Brugerorganisationer kan tilslutte en lokal IdP instans til NemLog-in og angive, at IdP'en må autentificere erhvervsidentiteter tilknyttet til brugerorganisationen. En bestemt lokal IdP instans kan godt håndtere flere brugerorganisationer, hvilket håndteres ved at IdP'en i NemLog-in tilknyttes en 'white-list' med specifikke CVR-numre, som IdP'en må autentificere brugere fra. Denne white-list håndteres af NemLog-in og konfigureres ifm. tilslutning af den lokale IdP.

Inden en lokal IdP kan kommunikere med NemLog-in, skal den tilsluttes, hvilket konkret sker via brugerfladen i MitID Erhverv. En brugerorganisation skal kontakte NemLog-in forvaltningen for at få tildelt en rettighed til kunne oprette en lokal IdP. Tildeling af rettigheden forudsætter, at den lokale IdP fremgår på NSIS positivlisten[3] og er anmeldt på mindst sikringsniveau Betydelig.



Figur 3: Oprettelse af lokal IdP i MitID Erhverv (prototype)

[3] https://digst.dk/it-loesninger/standarder/nsis/

4.3 NemLog-in's miljøer

NemLog-in har to primære miljøer[4], hvortil en lokal IdP-instans kan tilsluttes og integreres:

- Et testmiljø (beta-testmiljø[5]), hvor integrationen mellem en lokal IdP og NemLog-in kan afprøves med testbrugere, testcertifikater og testdata. Snitfladen vil funktionelt være den samme som i produktionsmiljøet, men i testmiljøet vil der være testudgaver af tjenesteudbydere, som man kan prøve at logge på gennem en lokal IdP.

- Et produktionsmiljø som alene håndterer 'rigtige' autentifikationer af erhvervsbrugere, som herefter tilgår tjenesteudbydere i produktion.

En lokal IdP skal som tidligere nævnt have fuldført anmeldelsesprocessen i NSIS, før den kan tilsluttes produktionsmiljøet i NemLog-in. Tilslutning til testmiljøet forudsætter imidlertid ikke, at den lokale IdP er NSIS anmeldt, hvilket gør det mulig at arbejde på NSIS anmeldelsen og den tekniske integration parallelt.

4.4 Certifikater og metadatafiler

Før der kan ske en sikker kommunikation mellem NemLog-in og den lokale IdP, skal der udveksles såkaldte SAML metadatafiler, som beskriver hver parts endepunkter, certifikater, og kapabiliteter i forhold til SAML.

En sikker kommunikation vil typisk opnås ved anvendelse af et FOCES eller VOCES-certifikat per instans af den lokale IdP (et testcertifikat til en instans, som rettes mod NemLog-in's testmiljø, og et produktionscertifikat til den instans, som rettes mod NemLog-in's produktionsmiljø). Bemærk, at FOCES/VOCES-certifikaterne erstattes med nye certifikattyper med tilsvarende funktionalitet – certifikatpolitikkerne er publiceret på certifikat.gov.dk.

Det er særdeles vigtigt at beskytte den private nøgle for disse certifikater, idet uvedkommende med adgang til nøglen vil kunne impersonere den lokale IdP overfor NemLog-in og den øvrige infrastruktur. Med andre ord vil man kunne signere en adgangsbillet og logge ind som en hvilken som helst erhvervsbruger i brugerorganisationen. Af denne årsag stiller NSIS på niveau Høj (og i visse tilfælde på niveau Betydelig), krav om hardwarebeskyttelse af den private nøgle. Det er således vigtigt, at brugerorganisationen nøje designer procedurer og driftsmiljø for den lokale IdP, så kravene til nøglebeskyttelse opfyldes.

4.5 Varianter af lokale IdP'er

Ved tilslutning af en lokal IdP er det overfor NemLog-in muligt at angive, at den lokale IdP er implementeret med et bestemt IdP produkt som fx Microsoft AD FS, Novell Identity Manager mv. Denne oplysning vil NemLog-in benytte til at tilpasse dele af kaldet til den lokale IdP, idet visse produkter har begrænsninger i forhold til understøttelse af SAML protokollen. Et eksempel på et område, der tilpasses, er kommunikation af ønsket NSIS sikringsniveau (se afsnit 4.8), hvor RelayState kan anvendes

[4] Der er dog flere miljøer som fx anvendes til beta- og pilotafprøvning.

[5] https://www.nemlog-in.dk/vejledningertiltestmiljo/

som supplement til AuthnContextClassRef elementet (se krav [OIO-SP-06] og [OIO-SP-07] i OIOSAML profilen for lokale IdP'er).

4.6 Lokal IdM-løsning

Det er som tidligere nævnt et krav til brugerorganisationer, at alle erhvervsidentiteter, som skal kunne føderes via NemLog-in, ligeledes bliver oprettet i MitID Erhverv. Vedligeholdelsen kan enten ske via en brugergrænseflade, som tilgås af en administrator, eller via IdM API'et udstillet af MitID Erhverv.

En lokal IdM løsning tilsluttes til NemLog-in via erhvervsløsningen på samme måde som en lokal IdP dvs. gennem brugerfladen i MitID Erhverv. Det er således muligt at teste en integration mod NemLog-in's testmiljø, inden der sker tilslutning til produktionsmiljøet.

For at en lokal autentifikation kan formidles gennem NemLog-in skal der være en overensstemmelse mellem Subject feltet i den udstedte SAML Assertion og en erhvervsidentitet oprettet i MitID Erhverv for den pågældende brugerorganisation[6]. Det er brugerorganisationens ansvar at sikre denne overensstemmelse, herunder opdatere oplysningerne i MitID Erhverv via IdM API eller brugerflade, hvis Subject NameID for en bruger ændres lokalt.

4.7 Attributter og rettigheder fra lokal IdP

En lokal IdP skal som minimum kunne levere de obligatoriske attributter, som fremgår af OIOSAML 3.0 profilens kapitel 6.

Der vil derudover blive defineret et NemLog-in-specifikt format, hvor den lokale IdP kan overføre en liste af gruppenavne til NemLog-in, som i NemLog-in ekspanderes til et sæt af rettigheder til den aktuelle tjenesteudbyder. Vedligeholdelsen af gruppedefinitioner (herunder deres tilhørende privilegier) sker i NemLog-ins brugerrettighedsstyring og defineres per brugerorganisation. Formatet for dette er endnu ikke endeligt specificeret, men vil være baseret på brug af OIO Basic Privilege Profile, hver de lokale grupper for brugeren angives som et sæt af URI'er.

Tjenesteudbyderen vil efter omvekslingen i NemLog-in modtage privilegier som beskrevet i OIO Basic Privilege Profile, og vil således ikke kunne se forskel på, om erhvervsbrugerne har fået privilegier tildelt centralt i NemLog-in eller lokalt via en gruppe, der i NemLog-in er omvekslet til privilegier.

4.8 Håndtering af NSIS sikringsniveauer i request

Hvis tjenesten, som ønsker autentifikation, har angivet ønske om et bestemt NSIS sikringsniveau til NemLog-in, videreformidles dette til den lokale IdP. Dog vil NemLog-in aldrig anmode om autentikation på et højere sikringsniveau, end IdP'en er anmeldt til. Den lokale IdP behøver ikke kunne honorere det forespurgte niveau for den aktuelle bruger, men skal altid angive det aktuelt opnåede NSIS sikringsniveau i svaret. Den lokale IdP skal derfor guide brugeren til at opnå det forespurgte sikringsniveau i den lokale autentifikation, idet brugere med utilstrækkeligt sikringsniveau ellers ville kunne få adgang til tjenesteudbyderen. Dette kan den eksempelvis gøre ved at afkræve to-faktor autentifikation, når det tjenesteudbyderen har brug for dette.

[6] På en erhvervsbruger i MitID Erhverv kan man angive det tilhørende lokale brugernavn (Subject NameID).

4.9 Forhold vedr. sessionsstyring

Ved implementering af en lokal IdP er det vigtigt at forholde sig til sessionsstyring, herunder single sign-on og single logout, samt dettes samspil med lokal sessionsstyring, der kan være etableret i brugerorganisationens domæne. Specifikt kan fremhæves følgende opmærksomhedspunkter:

- Det er i udgangspunktet tilladt at basere autentifikationen i den lokale IdP på en allerede-eksisterende brugersession fra domænet, så længe NSIS-kravene på det aktuelle sikringsniveau overholdes. Dog skal brugeren eksplicit afkræves autentifikation, hvis ForceAuthn flaget er sat i forespørgslen fra NemLog-in (se OIOSAML profilen).

- Hvis NemLog-in anmoder den lokale IdP om single logout, er det tilstrækkeligt at fjerne al sessionsinformation (cookies etc.) fra den lokale IdP i brugerens **browser**. Det er således acceptabelt, hvis brugerens browser via den underliggende session på det lokale domæne kan forhandle en ny session uden aktiv brugerinvolvering. Single logout går altså på IdP-sessionen i browseren, men ikke nødvendigvis på pc'ens session med det lokale domæne.

4.10 Konfiguration af kryptografiske algoritmer

De fleste SAML IdP produkter skal konfigureres med de kryptografiske algoritmer og nøglelængder, der dels bruges på transportlaget og dels ved kryptering og signering af SAML Assertions. Her er det vigtigt at være opmærksom på, at OIOSAML profilen stiller krav til de anvendte algoritmer og nøglelængder (kapitel 3.3), hvilket betyder, at svagere algoritmer og nøglelængder skal slås fra i konfigurationen af produktet.

Dette gælder også TLS, hvor der skal anvendes mindst version 1.2 eller højere, og hvor ældre (og sårbare) versioner dermed skal slås fra.

4.11 NSIS-krav til lokal IdP

Ud over kravene i OIOSAML-profilen til den lokale IdP'er er det vigtigt at være opmærksom på de krav, som fremgår i NSIS kapitel 6. Disse omfatter bl.a.:

- Krav til beskyttelse af den private nøgle, som underskriver SAML Assertions – herunder procedurer for nøglehåndtering.

- Krav til sessionsbeskyttelse.

- Krav til logning af forespørgsler og svar til/fra IdP'en til en integritetsbeskyttet log.

- Brug af AudienceRestriction i udstedte Assertions.

- Kryptering af tokens med følsomt indhold.

5. Trin-for-trin implementeringsguide

Nedenfor er beskrevet de typiske trin, der indgår i etablering og tilslutning af lokal IdP. Beskrivelsen dækker både implementering af NSIS og integration via OIOSAML 3.0. Trinene er af hensyn til overskueligheden forsimplede, og der vil i den enkelte implementering naturligt være langt flere detaljer, som skal håndteres.

1. Afklar ønsker og forretningsmæssige behov for lokal IdP herunder NSIS sikringsniveau for de tjenester, som ønskes tilgået. Dette indikerer, om erhvervsbrugerne skal kunne autentificere sig på niveau Betydelig eller Høj (eller evt. opdel erhvervsbrugere i forskellige grupper med forskellige behov). Ligeledes afklares krav til oppetid, svartider og andre servicemål[7] for lokal IdP, så implementeringen kan modsvare forretningsmæssige behov. Overvej endvidere hvordan lokale erhvervsidentiteter provisioneres til NemLog-in; skal der laves integration mellem lokalt IdM system og NemLog-in eller ønsker man at anvende NemLog-ins webportal til administration af erhvervsidentiteter.

2. Etabler projekt og skab ledelsesopbakning.

3. Foretag gap-analyse, som sammenholder NSIS krav på det ønskede sikringsniveau med nuværende processer og systemer. Dette omfatter bl.a. følgende:

    a) Identificér ønsket proces for identitetssikring. Skal erhvervsbrugerne fx første gang logge på med privat MitID og sker dette i lokal indrulleringsapplikation eller centralt i NemLog-in, eller skal erhvervsbrugerne i stedet møde fysisk op og præsentere pas/kørekort mv.

    b) Afklar hvilken type identifikationsmidler, der skal udstedes lokalt, og hvordan de udleveres og håndteres. Typisk kombineres et brugernavn og kodeord med ekstra faktorer på særlige hardwareenheder, fra apps på mobile enheder mv.

    c) Afklar hvordan autentifikationsservicen etableres teknisk (IdP), og hvordan den kan understøtte de valgte sikringsniveauer. Den lokale IdP skal som nævnt udstille en SAML snitflade, som opfylder kravene i 'OIOSAML Local IdP Profile'.

    d) Afklar krav til driftsfaciliteter og teknisk sikkerhed. Er nuværende driftsfaciliteter modne nok, eller skal der ske forbedringstiltag?

    e) Afdæk behov for uddannelse af erhvervsbrugere, der skal arbejde med fx identitetssikring eller andet.

[7] Bemærk at NemLog-in ikke stiller krav til servicemål for lokal IdP, så det er brugerorganisationens egne behov, der skal afdækkes.

f) Etabler ledelsessystem for informationssikkerhed (ISMS) eller tilpas eksisterende, så det dækker processer for identitetshåndtering.

g) Afklar håndtering af underleverandører af fx software eller drift, som leverer dele af den lokale implementering.

h) Beskriv processer, sikkerhedsdesign og tekniske systemer og få design reviewet.

i) Planlæg hvordan systemer og processer kan auditeres af ekstern revisor. Det er fx vigtigt, at der sikres et tilstrækkeligt revisionsspor, så revisor kan konstatere, at processer, personer og systemer udfører de kontroller, som er tiltænkt.

4. Implementér nødvendige systemer og processer i henhold til ovenstående.

   a) Etablér miljøer til lokal IdP og tilhørende brugerkatalog, og etabler de nødvendige komponenter og services.

   b) Anskaf nødvendige certifikater til den lokale IdP.

   c) Foretag lokal test herunder både funktionel test og sikkerhedstest.

   d) Gennemfør test af organisatoriske processer

5. Foretag testtilslutning mod NemLog-in og afprøv lokal IdP i betatesttestmiljø[8].

6. Indhent nødvendige revisionserklæringer og ledelseserklæringer til brug for NSIS-anmeldelse. Tidlig dialog med revisor kan anbefales.

7. Indsend anmeldelsespakke (inkl. revisionserklæringer) til NSIS tilsynet i Digitaliseringsstyrelsen og afvent godkendelse / supplerende spørgsmål.

8. Efter godkendelse send mail til NemLog-in's Forvaltning, og anmod om at rettigheder tildeles til brugerorganisationen jf. den godkendte NSIS-anmeldelse.

9. Efter rettigheder er tildelt, kan den lokale IdP tilsluttes NemLog-in's produktionsmiljø af Organisationsadministrator via MitID Erhverv, og herefter er den live og tilgængelig for autentifikation

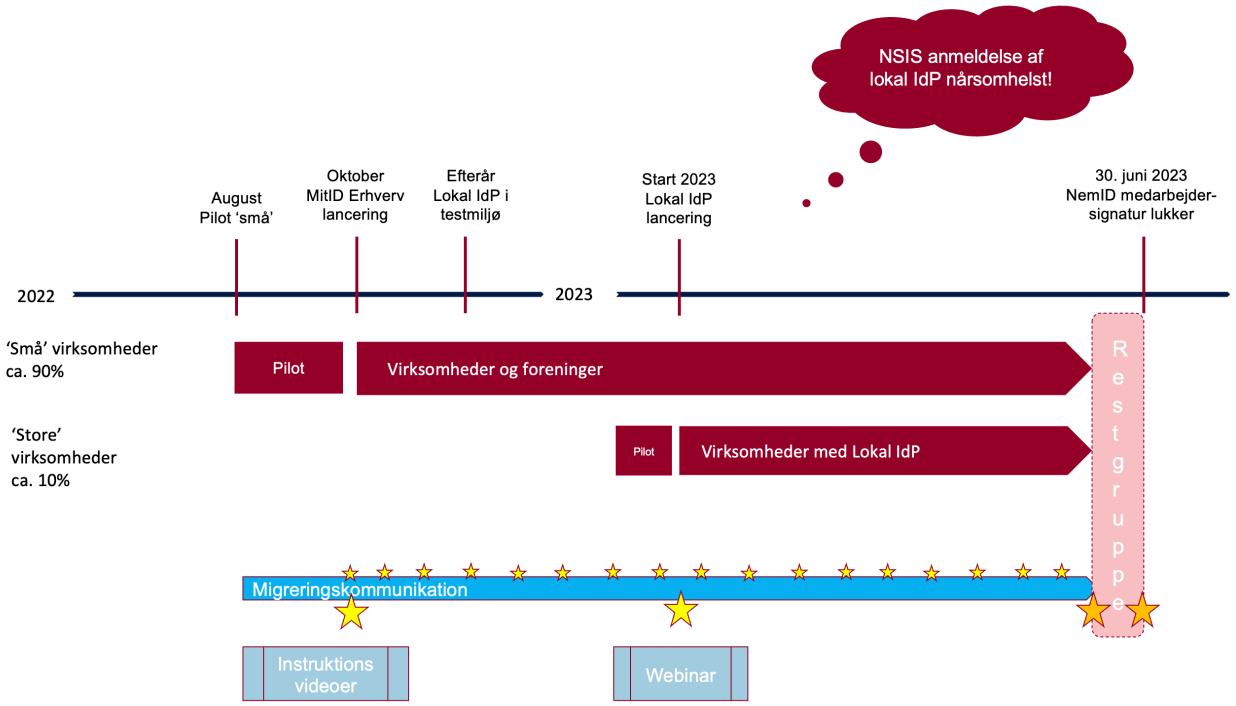
Hvis der skal laves integration med lokalt IdM system, skal dette også på plads.

[8] https://www.nemlog-in.dk/vejledningertiltestmiljo/

6. Tidslinje

Tilslutning af lokale IdP-løsninger for brugerorganisationer forventes at kunne ske i produktion primo 2023, mens tilslutning til NemLog-in's testmiljøer er muligt fra oktober 2022. IdM API snitfladen er gået i produktion oktober 2022 med første release af MitID Erhverv.

Der må påregnes en ikke uvæsentlig indsats med at implementere NSIS, etablere det tekniske setup for IdP/IdM, samt indhente de nødvendige revisionserklæringer. Det kan derfor klart anbefales at starte i god tid inden de nævnte datoer. NSIS anmeldelse kan ske i god tid inden, man har behov for at gå produktion.



Bemærk at NemID nedlukkes med udgangen af juni 2023, hvorfor alle organisationer, der ønsker at anvende lokal IdP skal have NSIS anmeldt og tilsluttet denne til MitID Erhverv inden.

7. Referencer

[OIOSAML] "OIOSAML Web SSO profile 3.0 SO profile 3.0" samt

"OIOSAML Local IdP Profile 1.0"

https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

[NSIS] "National Standard for Identiteter Sikringsniveauer 2.0.1a".

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

Læs mere om MitID Erhverv på: https://digst.dk/it-loesninger/standarder/nsis/

Læs mere om testmiljøet på: https://digst.dk/it-loesninger/standarder/nsis/ herunder dokumentation og eksempelkode for IdM API'et.