Delrapport 2 fra KL om

National Standard for Identiteters Sikringsniveau (NSIS).

Version: 1.1
Udgivet: 16. februar 2022
Udgiver: Vangsaa Consult ApS, på bestilling af KL.

VANGSAA CONSULT

Indhold

Ledelsesresumé

Danske myndigheder og virksomheder lever i hverdagen med truslen om at blive udsat for kriminalitet med afsæt i vores brug af IT. Center for Cybersikkerhed gik i 2021 så langt som til at sige, at det ikke længere er et spørgsmål, **om** vi bliver ramt. Det er et spørgsmål om, **hvornår** vi bliver ramt.

Det trusselsbillede gør det nødvendigt at sætte ekstra fokus på at sikre informationer om borgerne og forretningen efter bedste evne. Det nedbringer risikoen for misbrug mv. Og det løfter borgernes tillid til kommunerne, som den nære offentlige myndighed i den enkeltes hverdag.

En del af det, er at havebedre styr på brugerkonti og -rettigheder, når der oprettes brugere, administreres rettigheder og nedlægges brugerkonti. Og at udelukkende at tildele rettigheder udfra arbejdsbetingede behov. Fremadrettet må det forventes, at adgang til oplysninger og konti i de kommunale systemer kommer til at bygge på mere sikre passwords og ofte suppleret af flerfaktor autentifikation.

Den rapport, du sidder med i hænderne eller på skærmen handler om forberedelsen til den fremtid. Og overholdelse af kravene i NSIS stiller netop krav, der er en del af sikringen ift. denne fremtid. Mange oplever kravene og aktiviteterne som store indgreb i handlefrihed og opgavetilrettelæggelse, Men det er bedre set som et boost til håndteringen af brugerstyring og den generelle modstandskraft overfor udefra kommende trusler eller angreb.

Denne rapport handler om kommunernes handlerum og opgaver i forbindelse med analyse, implementering og drift, hvis man vælger en lokal IdP, der så skal overholde National Standard for Identiteters Sikringsniveau (NSIS) lokalt i hver kommune i forbindelse med, at der indføres den fællesoffentlige føderation *NemLog-in3* ved overgang fra *NL2* med NemID til MitID.

Rapporten kommer med et bud på, hvilke opgaver der kan igangsættes i kommunen, og som bør gå forud for anskaffelse og implementering af en lokal IdP.

Kommunen kommer til at arbejde mere målrettet med *compliance*, og det kan afføde organisatoriske tilpasninger og justeringer. Kommunerne anbefales derfor at opfatte opgaven og arbejdet omkring NSIS som en mulig løftestang til styrkelse af arbejdet med compliance helt generelt i organisationen.

Compliance arbejdet forventes særligt omfattende hos de kommuner, som vælger at udvikle en IdP selv, fordi der er skærpede krav til, hvordan udvikling styres fra idefase til slutprodukt i produktion. I hele processen skal revisionsspor tænkes med ind i forhold til *NSIS-krav*. Det vil sige krav til udvikling, test herunder penetrationstest, risikovurderinger i forhold til trusselsbillede mv. Beskyttelse skal være tænkt med ind i udviklingen, og security by design som også GDPR foreskriver. Hvordan dokumenteres dette?

KL vil som opfølgning på denne rapport etablere et ERFA-netværk, hvor kommunerne indbydes til at deltage. I netværket vil der fra KL blive faciliteret yderligere videns udveksling og komme løbende opdateringer vedr. NSIS arbejdet.

Læsevejledning

Rapporten indeholder et bilag 2, hvor det er muligt at finde ordforklaring og definitioner som anvendes i rapporten. Derudover vil der også i bilag 2 være link henvisninger med kort forklaring til, hvad der findes via linket.

I rapporten vil alle ord der er skrevet med *kursiv og understreget*, skulle opfattes som en henvisning til bilag 2 for uddybende forklaring samt evt. link til eksempelvis relevant vejledning hos Digitaliseringsstyrelsen.

Markeringen af ord som henviser til bilag 2, sker første gang ordet eller definitionen anvendes.

Det er derudover vigtigt at være opmærksom på, at i forlængelse af "ledelsesresumé" kommer der en opsummering af anbefalet tidslinje med beskrivelse af arbejde og anbefalinger. Rapporten kommer først i dybden med mere specifikke beskrivelser efter kapitlerne "ledelsesresumé" og "Foreslået tidslinje og implementering i kommunerne".

Målgruppe for rapporten

KL ønsker med denne rapport at henvende sig til

- it-chefer
- it-arkitekter
- programledere, projektledere og projektdeltagere
- og andre relevante interesserenter,

der arbejder med kommunens implementering af NSIS.

Sammenhæng til delrapport 1

Denne rapport ligger i naturlig forlængelse af delrapport 1 "*Kommuner som tjenesteudbydere og nye krav fra NSIS*", som KL udgav i april 2021.

Indhold i delrapport 2

Arbejdet med NSIS i kommunerne er omfattende og komplekst. Kommunerne er dygtige til og har stor erfaring med at arbejde med tekniske opgaver og projekter. Men NSIS-arbejdet stiller nye og skærpede krav til, hvordan man som kommune arbejder med compliance i relation til NSIS og i forhold til informationssikkerhed generelt.

Der bør derfor i de enkelte kommuner være et helt særligt fokus på den organisatoriske indvirkning, der kan være ved at arbejde med NSIS og med implementeringen af systemer og tekniske løsninger, som vil påvirke organisationen på en måde og i et omfang som i kommunerne ikke er vant til.

Der findes i denne rapport en række betragtninger, som det anbefales kommunerne at orientere sig i, og med udgangspunkt i disse vurdere, hvordan kommunerne selv ønsker at agere på den baggrund. Derudover findes der en række anbefalinger og forslag til tidsplaner og spor/projekter, der bør etableres for det videre arbejde med NSIS.

De to fokusområder i delrapport 2 er lokal IdP og ekstern brugerstyring i de TU-løsninger kommunernes ansatte tilgår i dagligdagen.

Lokal IdP i kommunerne

Den enkelte kommune har reelt 3 valgmuligheder i forhold til hele NSIS-området, når det handler om brugerstyring i kommunen.

1) Anvende den fællesoffentlige IdP løsning ude i *NL3*
2) Købe en lokal IdP løsning
3) Selv bygge og udvikle en lokal IdP løsning

Ved løsning 1 er det eksempelvis ikke muligt at anvende *manuel indrullering*, da Digitaliseringsstyrelsen ikke tilbyder dette i deres løsning. På den positive side slipper kommunen for at skulle udarbejde revisionserklæringer.

Vælger man løsning 2 eller 3 ovenfor stilles der en række NSIS-krav til kommunen. Dels til den tekniske løsning, dels til kommunens organisation. Højst sandsynligt minder de tekniske opgaver om opgaver, kommunen har arbejdet med før, men den organisatoriske del af arbejdet vurderes som en helt ny opgave. Den tekniske løsning, der vælges, vil i høj grad have indflydelse på omfanget af de opgaver, der skal løses i organisationen.

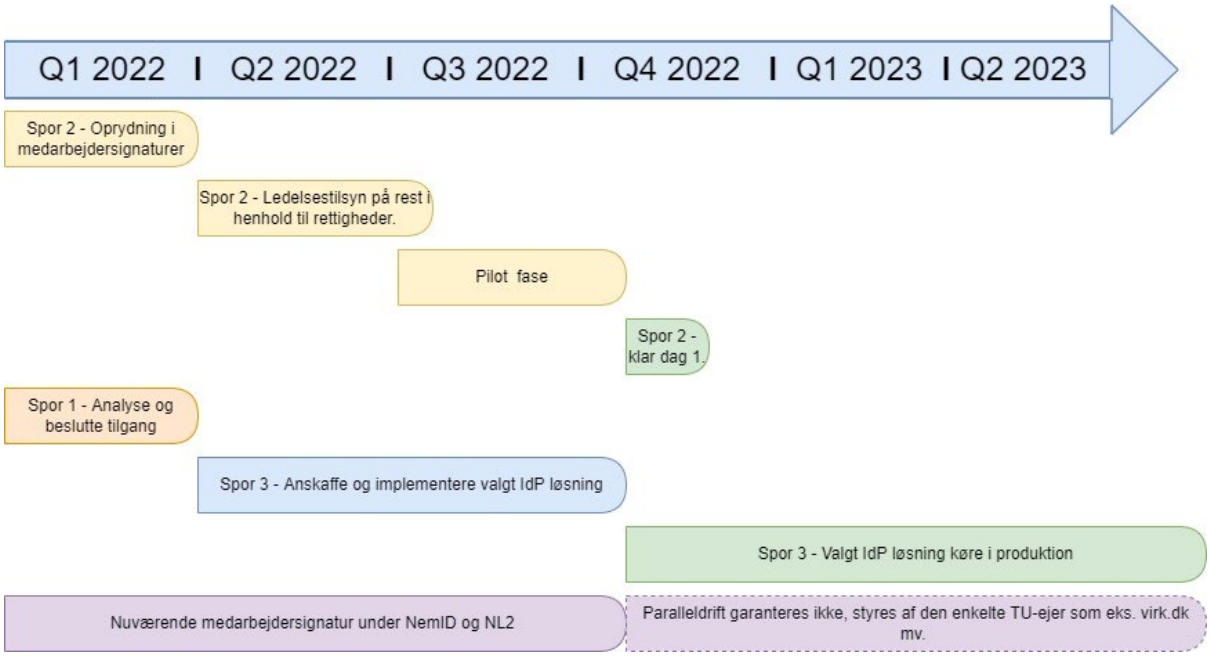
Uanset om man ovenfor vælger løsning 1, 2 eller 3, skal man som kommune forholde sig til, hvordan den interne brugerstyring fremadrettet skal håndteres. Yderligere om fordele og ulemper ved de enkelte valg er beskrevet nærmere på side 11.

Fællesoffentlige løsninger – ekstern brugerstyring i andres TU-løsninger

Hvis kommunen vælger at etablere en lokal IdP og tilslutte den til MitID Erhverv, og bruge den fra start, så anbefales det at kommunen påbegynder opgaven i umiddelbar forlængelse af, at den lokale IdP er etableret.

Konkret er der tale om, at kommunen anvender en række fællesoffentlige portaler som Fælles Medicinkort (FMK), virk.dk m.fl., hvor der skal oprettes medarbejdere, når de overgår til en ny erhvervsidentitet og deres nuværende *medarbejdersignatur* lukkes. Her er det vigtigt at kommunerne sikrer at RID påføres den nye *erhvervsbruger* for at der kan ske en automatisk omlægning af rettighederne fra den gamle medarbejdersignatur til den nye erhvervsbruger.

Foreslået tidslinje over kommunens implementeringsforløb



På de efterfølgende sider findes diagrammer pr. spor med overblik over de vigtigste opgaver, som skal igangsættes og løses i perioden januar 2022 til og med marts 2023.

Spor 1 – analyse og beslutte målbillede

Spor 1 dækker de organisatoriske og tekniske behov ved valg af en IdP løsning. Det er her vigtigt ikke at glemme de organisatoriske udfordringer, der kan opstå ved valg af den tekniske løsning.

Spor 1 skal munde ud i et *målbillede* og en anskaffelsesplan som ledelsen godkender inden udgangen af marts 2022.

Januar og februar 2022

Her skal kommunen arbejde med tekniske, organisatoriske og fleksible NSIS-kontroller, som du kan læse mere om på side 8 og i detaljer på side 15. Kommunen skal beslutte om der ønskes manuel, digital, eller begge former for indrullering og oprettelse af identitetsmidler. Vurder og beslut hvordan kommunen ønsker at håndtere 24/7 support, vitterlighedsvidner mv. Kort sagt, definer målbilledet med vægt på de organisatoriske muligheder. Brug afsnittet ”Introduktion til typer af NSIS-krav” på side 15 som tilgang til arbejdet.

Marts 2022

Besluttet målbillede ledelsesgodkendes.

Spor 2 – Ledelsestilsyn og omlægning af medarbejdere i eksterne løsninger

Spor 2 kan afvikles stort set uafhængigt af spor 1 og 3. Spor 2 er først afhængig af, at der er idriftsat en IdP løsning i kommunen for gennemførsel og omlægning af rettigheder i Q4 2022 og Q1 2023.

De bruger og rettighedsansvarlige i kommunen skal i denne periode identificere hvilke fællesoffentlige løsninger som FMK, virk.dk mv der anvendes af kommunens ansatte.

Kommunen skal nu ud i henholdsvis Scenarie A eller Scenarie B beskrevet på side 22 i forhold til de enkelte fællesoffentlige løsninger i spor 3.

Første halvår samt Q3 i 2022

Gennemfør et ledelsestilsyn, som sikrer, medarbejderne står med de rigtige rettigheder og at inaktive medarbejdere med en medarbejdersignatur slettes.

Arbejdet med at identificere og registrere rettigheder i alle de fællesoffentlige løsninger kan være omfattende.

Denne periode kan også med fordel bruges på dialog med de myndigheder, der har fællesoffentlige TU-løsninger, for at identificere om scenarie A eller B, beskrevet på side 22, er relevant for den enkelte myndighedsløsning som virk.dk, FMK mv. Det vil have stor betydning for arbejdets omfang, om det er scenarie A eller B, der er beskrevet på side 21.

Q4 2022 samt Q1 2023

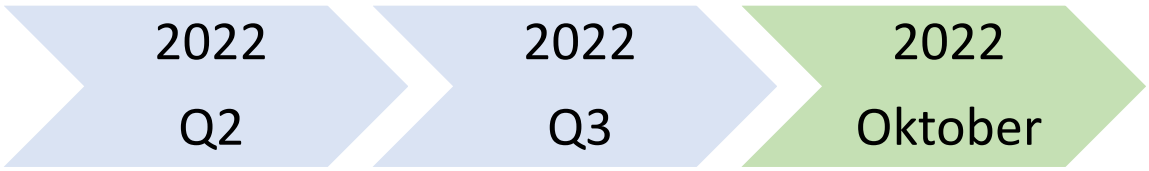
Kommunen skal nu ud i de henholdsvis Scenarie A eller scenarie B i forhold til de enkelte fællesoffentlige løsninger.

Der skal omlægges brugere og rettigheder fra den gamle medarbejdersignatur til den nye erhvervsbruger under MitID.

Opgaverne skal løses pr. fællesoffentlige løsning, som det tidligere er identificeret.

Spor 3 – Implementering og idriftsættelse

Spor 3 bygger videre på arbejdet i spor 1 og skal sikre implementering og idriftsættelse af en IdP løsning i kommunen. Spor 2 kan først fortsætte den sidste del af omlægningen, når spor 3 er afsluttet.



Q2 2022

Indkøb af den tekniske løsning skal nu gennemføres. Det kan ske på baggrund af det målbillede der er opsat i spor 1 kombineret med øvrige ønsker til funktionalitet og organisatorisk implementering.

I Q2 bør der ske anskaffelse af ønsket løsning.

Q3 2022

Fokuser på implementeringen og udarbejd de processer og procedurer, der skal understøtte den tekniske og organisatoriske NSIS-compliance.

På de NSIS-kontroller, hvor en leverandør løser kravet, skal der modtages en revisionserklæring fra leverandøren ultimo Q3. Digitaliseringsstyrelsen accepterer, at en revisionserklæring fra en leverandør er indtil 12 måneder gammel, når den anvendes som en del af det grundlag, der er for udarbejdelse af kommunens egen erklæring for den lokale IdP. Digitaliseringsstyrelsen forlanger dog, at den erklæring kommunen udarbejder ikke er mere end 90 dage gammel, når den lokale IdP anmeldes til Digitaliseringsstyrelsen.

Det er også her i Q3 revisoren skal deltage i arbejdet, for at der kan være en påtegnet revisionserklæring klar i oktober 2022.

Opmærksomhedspunkter og opgaver i regi af de 3 spor:

Når der arbejdes med de 3 spor som illustreret, kan en eller flere af nedenstående punkter være relevante at medtage i overvejelserne.

1) Opstil kravene fra spor 1 i et NSIS-målbillede. Målbilledet skal danne rammen for, hvilke udpegede kontroller kommunen skal følge. Det skal dokumenteres hvilke kontroller, der forankres teknisk og som dermed skal være krav til den løsning, der etableres. Derudover skal de NSIS-kontroller, der forankres som manuelle kontroller (forankring i organisationen), tilsvarende dokumenteres. I processen er det vigtigt at beslutte, hvor de fleksible kontroller forankres som beskrevet i afsnittet ”Introduktion til typer af NSIS-krav” på side 15. Med udgangspunkt i dokumentet er der nu et overblik over hvilke krav, der skal stilles til indkøb eller egenudviklet løsning. Derudover er der nu en tilsvarende liste over de kontroller, som skal forankres i kommunens organisation omkring den lokale IdP løsning. Det vil sige, at kravene nu kan konverteres til konkrete opgaver i organisationen.

2) Infrastrukturen i dag bygger på virksomheds-, funktions- og person-certifikater. I den nye infrastruktur under Nem Login3, vil det ikke være muligt at anvende personlige certifikater. Kommunen skal undersøge, om der er områder eller løsninger i kommunen, som anvender dette. I det omfang disse certifikater findes i dag, skal kommunen beslutte hvordan disse udfases og nye løsninger indføres.
3) Kommunen bør undersøge, om der i integrationer i egne systemer anvendes virksomheds- eller funktions-certifikater. De steder, hvor disse anvendes, skal der fremover bruges virksomhedscertifikater fra Nem Login3.
4) NSIS-krav 4.1.3 stiller krav om, at kommunen med en lokal IdP på sikringsniveau Betydelig, skal etablere et effektivt ledelsessystem for informationssikkerhed (ISMS). Dette skal dække den lokale IdP med henblik på at håndtere risici knyttet til informationssikkerhed, samt at ledelsessystemet følger principperne i ISO27001. Det vil sige, at der konkret skal være et trusselsregister for den lokale IdP, som det dokumenteres er håndteret og løftet i den IdP-løsning, der indkøbes eller bygges af kommunen selv. Der skal være en beredskabsplan, som sikrer driften af den lokale IdP, og beredskabsplanen skal kunne håndtere alle væsentlige områder. Det vil sige, at beredskabsplan eks. skal dække de trusler, der på baggrund af en risikovurdering udgør en risiko for den lokale IdP. Tænk både den lokale IdP i sig selv og de brugsscenarier, der er hos brugerne tilknyttet den lokale IdP.
5) Overvej tilsvarende om der skal være et separat målbillede for børn og unge området og skolernes behov for en tilsvarende IdP løsning.
6) *NSIS-rammen* og de medfølgende compliance krav fokuserer alene på identifikation af en medarbejder. Det er i den forbindelse vigtigt at huske på, at KOMBITs Contexthandler ikke løfter compliance-krav i kommunen til indrullering og identifikation af de ansatte i en IdP løsning. Der er primært fokus på rolle og rettighedsstyring som ikke reguleres af NSIS. Med tiden, efterhånden som modenhed og erfaring vokser, kan man overveje frivilligt at udvide anvendelsen af NSIS-rammen til systemer, som det ikke er obligatorisk at inkludere. Alt andet lige vil det formentligt øge dokumentationskravene og omkostningerne relateret til de systemer, man frivilligt vælger at inkludere i NSIS-rammen. Omkostningerne forbundet til at indrullere flere systemer frivilligt under NSIS, skal også holdes op mod, om man får mere sikkerhed for de samme penge med en mere klassisk tilgang til informations og cybersecurity generelt, frem for at fokusere ensidigt på NSIS som kun regulerer identifikation af en bruger.
7) Bemærk, at den lokale IdP i kommunen skal være klar til pilot-drift i sommeren 2022 hvis kommunen har besluttet at anvende lokal IPDIgangsætning til produktion forventes at ske 22. oktober 2022.
8) Det anbefales, at kommunerne i god tid overvejer, hvilken betydning identifikation af vikarer har for samarbejdet med vikarer og vikarbureauer. Skal der opstilles særlige NSIS-krav ved udbud af vikarydelser for at sikre, at vikarer enten allerede er indrulleret eller der er sket andre tiltag forud for en start på vagt. For at undgå problematikken med vikarer, kan man også beslutte, at det kun er fastansatte, der må have adgang til eksempelvis FMK med deres medarbejdersignatur. På den måde kan man organisatorisk arbejde uden om vikarudfordringen i den kommende lokale IdP løsning. Men det kan kræve en organisatorisk omlægning og anderledes planlægning af hvem, der er på arbejde i dagligdagen. Hvis man har tilvalgt muligheden for manuel indrullering, hvordan sikres det så med 24/7 support ude på de enkelte arbejdspladser?
9) Den første og vigtigste opgave i kommunen for at bevare et overblik er, at dokumentere kontroller i et samlet dokument. Dokumentet anbefales etableret på baggrund af *Digitaliseringsstyrelsens kontrolark til revisionserklæring*. Arbejdet skal ses som etablering af

målbilledet for den valgte IdP-løsning. Digitaliseringsstyrelsen kontrolark opdateres i første omgang ved at slette de kontroller, som ikke er relevante for kommunen. Dermed får kommunen et udgangspunkt for det, der skal leves op til. Herefter kan dokumentet bruges til styring af, at kommunen har løst alle kontroller og forpligtigelser. Målbilledet vil også være et godt værktøj at bruge i samarbejdet med revisor, når selve revisionserklæringen skal udarbejdes.

10) Den enkelte kommune skal identificere alle de fælles offentlige løsninger, der anvendes. Der er i Bilag 1 en liste til inspiration med fællesoffentlige løsninger, som kan være relevante at overveje hos den enkelte kommune.

Valg af lokal IdP og mulige tilgange – spor 1 og 3

Som tidligere nævnt er der tre valgmuligheder vedr. valg af lokal IdP.

1) Anvende den fællesoffentlige IdP løsning ude i NL3
2) Købe en lokal IdP løsning
3) Selv bygge og udvikle en lokal IdP løsning

Fordele og ulemper ved den fællesoffentlige IdP

Nedenfor skitseres kort fordele og ulemper ved at vælge den fælles offentlige løsning fremfor en lokal IdP løsning. Listen er ikke udtømmende, og der medtages oplysninger omkring Contexthandler, hvor det vurderes relevant.

Fordele ved den fælles offentlige IdP:

1) Digitaliseringsstyrelsen tilbyder *digital indrullering* i løsningen
2) Man kan købe tokens til de ansatte, hvor der skal bruges 2 faktor login.
3) Hvis ansatte har en mobil enhed, kan man også anvende APP som anden faktor.
4) Det dobbelte frivillighedsprincip – ansatte kan bruge privat MitID i arbejdsøjemed.
5) Der spares udgifter til revisionserklæring.
6) Der skal ikke etableres NSIS compliance i kommunen, da dette håndteres af Digitaliseringsstyrelsen via den fællesoffentlige IdP.

Ulemper ved den fællesoffentlige IdP løsning:

1) Man får ikke single sign-on (SSO), som der er i dag mellem den kommunale bruger og medarbejdersignaturen. For de kommunale medarbejdere betyder det mere spildtid og support ved login udfordringer.
2) Man kan ikke gennemføre manuel indrullering.
3) Man kan ikke individuelt i kommunen styre timeout, når man er logget på. Dette styres af Digitaliseringsstyrelsen i den fællesoffentlige IdP.
4) Man skal anvende de loginmidler Digitaliseringsstyrelsen tilbyder og kan ikke anvende dem, kommunen har allerede. Øgede omkostninger til login midler.
5) Man skal muligvis indkøbe flere enheder (mobil/tablet) i det omfang, man ønsker at bruge MitID app som 2 faktor.

Lokal IdP - valget mellem en købeløsning eller at bygge selv løsning

Her er det vigtigt at forholde sig til dels kommunens samlede IT-strategi, og dels hvor man som kommune gerne vil hen på sigt (10 til 12 år). Derudover skal man i kommunen kigge på egen modenhed i forhold til det at drive en række compliance-opgaver med revision, som skal dokumenteres og afleveres til Digitaliseringsstyrelsen årligt.

Relevante overvejelser er:

- On premise versus hosted
- Egen styring versus managed service
- Indkøbt eller selv byg
- Revisionserklæring på løsningen bredt både i kommunens IT-drift og organisation

- Skal det kun være digital indrullering eller også manuel indrullering af ansatte i den lokale IdP
- Hvordan håndterer kommunen vikarer, indrullering nu og her
- Indkøb af IdP er langsigtet. NemLog-in3 eksisterer de næste 10 til 12 år
- Skal der bruges mere end en IdP?
- Hvordan sikres det, at de fællesoffentlige standarder understøttes i valgte løsning

Det er vigtigt at gøre sig klart rent forretningsmæssigt og strategisk, hvad man ønsker af en eller flere lokale IdP løsninger. Eksempelvis om den skal understøtte, at man kan indrullere medarbejdere manuelt, fordi de ikke kan eller ønsker at anvende deres NemID eller fremtidige MitID til digital indrullering.

Manuel indrullering er et af de vigtige elementer, hvor kommunen skal vurdere, om det skal kunne ske, eller om man baserer sig på en ren digital indrullering. Manuel indrullering vil sige, at medarbejdere kan møde op fysisk i kommunen med deres pas eller tilsvarende og lade sig identificere som et led i indrulleringen i kommunens lokale IdP.

At medtage manuel indrullering som en option i sin løsning øger NSIS kravene væsentligt til kommunen, hvorfor det her eksempelvis giver god mening at sikre, at leverandøren har ansvaret for at løfte NSIS kravene, hvor det er muligt. Det kan medvirke til at minimere NSIS påvirkningen i organisationen. Herunder fjerne en stor administrativ opgave samt minimere omkostningerne til revisionserklæringen samlet set i kommunen. Køber man som kommune en lokal IdP løsning, som ikke understøtter manuel indrullering, så skal kommunen overveje at købe et system, der håndterer dette eller sikre, det sker manuelt i kommunen. Tilsvarende skal det sikres, at den løsning, der vælges, er revisor godkendt, samt at der til løsningen tilbydes den NSIS pligtige uddannelse af arbejdet med identitetspapirer og dokumenter.

I de efterfølgende sider kommer rapporten nærmere ind på muligheder, overvejelser og anbefalinger til valg af en lokal IdP.

Bemærk endvidere at den lokale IdP i kommunen skal være klar til pilot-drift i sommeren 2022, hvis man ønsker at deltage i pilotfasen. Igangsætning til produktion forventes at ske ultimo oktober 2022.

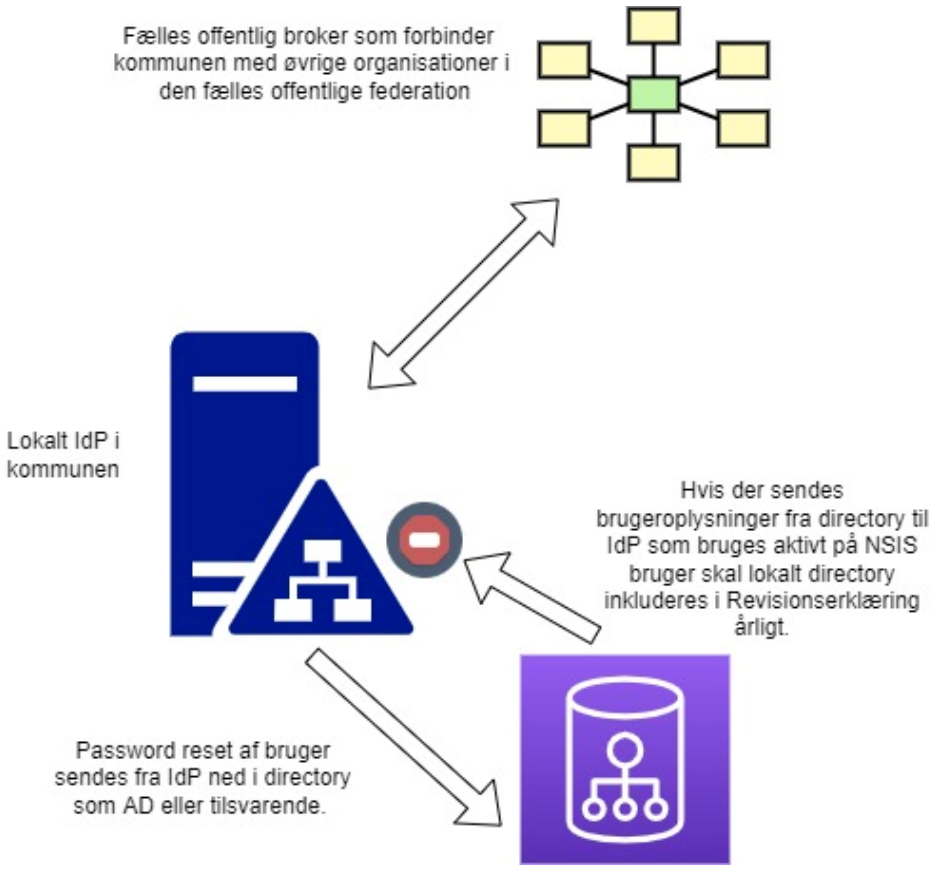
Det anbefales at starte op hurtigst muligt for at udnytte alle seks måneder i overgangsperioden til omlægning af brugere og rettigheder i fællesoffentlige løsninger som FMK, virk.dk m.fl.

Skematisk kan fordele og ulemper for de tre valgmuligheder opstilles således.

	Lokal IdP via leverandør	Fælles offentlig IdP	Driftet IdP i kommunen uanset om den er købt eller egenudviklet.
NSIS-compliance i kommunen	Ja – delvist	Nej	Ja – alt i NSIS-rammen
SSO	Ja	Nej	Ja
Udarbejde revisionserklæring	Ja - delvist	Nej	Ja på alt i NSIS-rammen.
Indrullering digitalt	Ja	Ja	Ja
Indrullering manuelt	Ja	Nej	Ja
Kommunen styrer timeout	Ja	Nej	Ja
Kommunen vælger identitetsmidler	Ja	Nej	Ja

I forhold til ovenstående diagram, hvor der skal vælges identitetsmidler til den lokale IdP løsning, er det vigtigt at huske på, at alt, der skal understøtte den lokale IdP, som udgangspunkt skal indgå i NSIS-compliance rammen.

For at kommunens lokale directory, eksempelvis AD eller AAD, ikke skal indgå i NSIS-compliance rammen, og dermed pålægge hele organisation at skulle overholde NSIS kravene, skal man derfor sikre integrationerne således.



Udfører kommunen password reset i det lokale directory på en bruger, som herefter synkroniseres op i den lokale IdP løsning, som skal være NSIS-compliant, så skal det lokale directory tilsvarende

overholde NSIS. Dette da det lokale directory nu vil være et bærende element på en af de faktorer, der indgår i NSIS-løsningen hos den enkelte bruger i det lokale IdP.

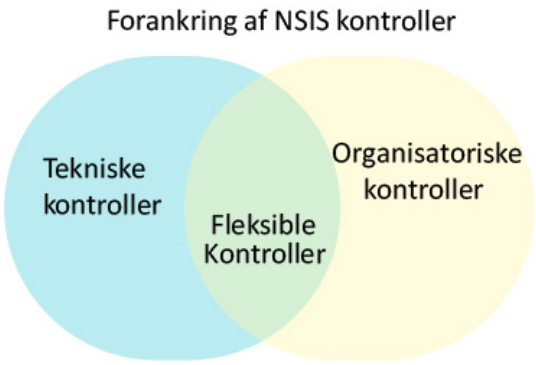
Det er derfor vigtigt at få afklaret, hvad revisoren vil acceptere og ikke acceptere i forhold til, hvad der skal medtages af kommunens infrastruktur i den samlede NSIS-erklæring.

Der kan muligvis være tekniske løsninger tilgængelige, som i en eller anden grad kan overføre oplysninger fra det lokale directory til NSIS-løsningen, som undtager det lokale directory fra NSIS-rammen. Disse er vi dog i skrivende stund ikke bekendte med.

Introduktion til typer af NSIS-krav

For at få en bedre indsigt i de muligheder og faldgruber, der er ved at vælge en IdP løsning, kommer her et kort indblik i typen af kontroller, der skal arbejdes med i kommunen omkring en IdP løsning.

Digitaliseringsstyrelsens dokument National Standard for Identiteters Sikringsniveauer (NSIS) findes som link i bilag 2



Når man arbejder med NSIS-kontrollerne i og omkring en IdP løsning, er det vigtigt at forholde sig til og beslutte, hvor NSIS-kontrollerne skal forankres.

De tekniske kontroller er kontroller, der i overvejende grad primært egner sig til en teknisk forankring i den IdP løsning, man vælger kommunen skal anvende.

Et eksempel på en teknisk kontrol kan være NSIS krav 3.2.1 Styrke af Elektronisk Identifikationsmiddel.

De organisatoriske kontroller er kontroller, som primært egner sig til implementering i kommunens organisation.

Et eksempel på en organisatorisk kontrol kan være NSIS krav 4.1.3 Informationssikkerhedsledelse.

De fleksible kontroller, er særligt interessante. Her er der mulighed for, at de kan placeres begge steder, og det er derfor vigtigt, at man som kommune forholder sig aktivt til denne gruppe af NSIS-kontroller.

Jo flere af disse ”fleksible” kontroller, der kan medtages i den tekniske løsning, jo billigere og nemmere bliver det for kommunen rent organisatorisk at være compliant. Særligt hvis det er en leverandør, der drifter og har ansvaret for løsningen. Så modtager man samtidigt som kommune en revisionserklæring fra leverandøren på alle de NSIS-kontroller, der er outsourcet.

Et eksempel på en fleksibel kontrol kan være 3.1.2 Verifikation af Identitet (fysisk person).

Her er der tale om, at der kan besluttes, at der skal ske en digital identifikation, hvor den lokale IdP skal basere sig på den ansattes personlige NemID eller fremtidige MitID i forbindelse med identifikationen.

Omvendt er det også muligt at foretage denne identifikation manuelt i kommunen. Her kommer dog en lang række krav, som skal overholdes, for at dette kan lade sig gøre. Der skal formelt etableres en intern løsning til de ansatte i kommunen, som svarer til det setup, der er i Borgerservice, når borgere skal have udstedt deres NemID eller fremtidige MitID.

Hvis kommunen ønsker at anvende manuel indrullering, vil det være meget relevant at afsøge leverandørmarkedet for IdP løsninger, som understøtter dette. Alternativt vil det være en tvungen opgave, som skal håndteres compliancemæssigt i kommunens organisation og formentligt kræve indkøb af andre systemer eller manuel indrulleringsramme. Herunder skal der investeres i NSIS-pligtig uddannelse af de ansatte for at arbejde med system / ramme for manuel indrullering af en medarbejder i den lokale IdP.

Der er mulighed for en vis synergi, når en medarbejder i kommunen arbejder i borgerservice og betjener borgerne, som skal have udstedt et MitID. Her kan den samme medarbejder bruges til at betjene ansatte i kommunen, som skal indrulleres manuelt i den lokale IdP. Forskellen vil dog være, at det ikke sker i Borgerservice via RA-portalen, men i et tilsvarende setup omkring den lokale IdP med selvstændigt system og udstyr til at scanne pas mv.

Modstykket til indrullering manuelt kan være at sikre, en digital løsning som understøtter indrullering digitalt via vitterlighedsvidner.

Når det er besluttet, hvor man ønsker NSIS-kontrollerne forankret og har identificeret de behov, der er, kan man afsøge markedet og sikre indkøb, der understøtter de krav, der er fra kommunens side til løsningen.

Andre overvejelser kan være, om det skal være en on premise-løsning, cloud-baseret løsning eller måske en managed service, hvor leverandøren leverer hovedparten af NSIS-kontrollerne, som en samlet løsning til kommunen.

Det anbefales endvidere, at kommunen tænker langsigtet, da et forkert valg de første år kan betyde, at der kommer ekstra omkostninger til i perioden. Eksempelvis at skulle ud og købe tillægs funktioner eller en helt ny IdP, hvilket vil minde meget om arbejdet og ressourcerne, der bruges i skiftet fra NemID medarbejdersignatur til erhvervsbrugeren under MitID. En ikke lille opgave.

Opgaven kort formuleret i punktform:

1) Gennemgå NSIS-krav og beslutte om de løftes teknisk, organisatorisk eller via begge,
2) Opstil alle kravene, som skal løftes af den tekniske løsning og indarbejd det i en kravspecifikation til indkøb og valg af den rette løsning.
3) Gennemføre indkøb og sikre implementering så løsningen er klar til produktion i perioden august til oktober 2022.

Vælger kommunen at bygge en lokal IdP, skal kommunen selv løfte og overholde kravsspecifikationen i forbindelse med udvikling, test og implementering af løsningen. I det efterfølgende afsnit kommer rapporten nærmere ind på muligheder og udfordringer ved at udvikle selv.

Når man har gennemgået punkt 1 og 2, har man indledningsvist målbilledet. Her skal dog justeres for særlige forhold, så man ikke utilsigtet øger licensomkostninger unødigt. Her er særligt børneområdet et fokuspunkt, når der skal træffes beslutning om en eller flere IdP løsninger i kommunen.

Opmærksomhedspunkter ved at bygge en lokal IdP løsning selv

Rapporten kommer i det efterfølgende med en tjekliste, som ikke er komplet, over de opgaver og overvejelser, man skal gøre sig i forbindelse udviklingen af en egen lokal IdP.

Først og fremmest skal kommunerne naturligvis gøre sig mange af de samme overvejelser uanset om man køber eller bygger selv. Skal der være en eller flere IdP løsninger? Skal kommunen bygge den centrale først, for så at tage en kopi til eksempelvis børne- og ungeområdet?

Det er ikke en ny teknologi, der skal opfindes, når man bygger selv. Der er en lang række komponenter, som muliggør, at man relativt simpelt kan udvikle en løsning, da det er gængs og kendt teknologi, som allerede anvendes flere steder.

Nedenfor kommer rapporten med en række overvejelser, som kommunen skal huske at gøre sig, hvis kommunen udvikler selv. De kommuner, der vælger at udvikle selv, har formentligt allerede

gjort sig mange af disse overvejelser og har dokumenteret disse som en del af forberedelsen til udarbejdelse af revisionserklæringen. Nedenstående skal derfor ses som en ekstra mulighed for at vurdere, om kommunen har været hele vejen rundt.

Nedenfor kommer eksempler på sikkerhedsmæssige, compliancemæssige og organisatoriske opgaver, der også skal huskes, og som går udover den rent tekniske opgave med at bygge løsningen.

- Hvordan løfter kommunen den NSIS-ramme, der henvises til i afsnittet "Introduktion til typer af NSIS-krav". Er det aktivt besluttet og dokumenteret hvilke krav, der skal løftes teknisk?
- Hvordan sikres et revisionsspor i IT-løsningen?
- Hvordan dokumenteres processer (brugsscenarier) og dataflow til ekstern revisor?
- Hvordan føres der tilsyn med driftsplatformen? Er det Ø-drift for at sikre, at krav ikke rammer hele IT-miljøet i kommunen?
- Hvordan kan relevante ISO27001/2 krav sandsynliggøres i den tilgang, der er til udvikling, test, testmiljø, produktionsmiljø mv.
- Hvordan beskyttes logs i produktion?
- Hvordan sikres funktionsadskillelsen i udviklingen, herunder krav til selve koden (udviklingsguide).
- Hvilke trusler fra kommunens trusselsregister og fra eksempelvis center for Cybersikkerhed er der taget højde for i udviklingen. Kan løsningen modstå risikobilledet, som er etableret på baggrund af en konkret risikovurdering forud for valg af tilgang til udviklingen.
- Hvordan sikkerhedstestes den samlede løsning for alle trusselscenarier, før den går i produktion. Security by design and by default (GDPR). Penetrationstest.
- Er der lagt en plan for, hvordan hele den tekniske løsning muliggør en ekstern revisor i at teste og kontrollere setup og løbende udføre stikprøver?
- Hvis løsningen hostes ude hos en 3. part, hvordan sikres de rigtige revisionserklæringer til at understøtte NSIS kravene og ISO27001/2 krav til driften?
- Hvordan håndteres en eventuel manuel indrullering af ansatte i en egenudviklet IdP løsning? Eller fokuseres der kun på en digital indrullering, som kan gøre løsningen mangelfuld i forhold til de organisatoriske behov, der er identificeret i kommunen.
- Hvordan udpeges relevante og konstruerede testdata, således der ikke anvendes "ægte" data i testcases og testmiljøer?
- Hvordan løfter kommunen til sikringsniveau Høj om eks. to eller tre år, hvis behovet opstår? Er dette behov tænkt med ind i det samlede design?
- Er der særlige krav til IdP løsningen for at kunne signere dokumenter? Snitflade, kald, logs?
- Hvilke integrationer skal der bygges ud til andre kommunale systemer? Hvordan sikkerhedstestes disse integrationer, kan disse systemer også afvikles i testmiljøerne sammen med den lokale IdP, således der kan gennemføres en fuld test som ligner produktion.
- M.fl.

Listen er ikke komplet, men er et hurtigt bud fra Vangsaa Consult på mulige opmærksomheds-punkter og opgaver, der skal favnes ved en egenudviklet IdP løsning. Mange af punkterne gør sig også gældende ved en købeløsning, eks. test i forhold til interne integrationer mv.

Ansatte på børne- og ungeområdet – skal de have egen lokal IdP?

I dag har mange kommuner adskilte AD-løsninger til området og har ikke skoleansatte og elever i deres centrale AD-løsning.

Grunden for denne tilgang kan være at finde i de licensvilkår, der er til uddannelsesområdet fra Microsoft. For at sikre de favorable uddannelseslicenser, skal området være isoleret fra den øvrige del af kommunen.

Det anbefales derfor, at kommunen nøje overvejer tilgang på området og om de beslutninger der træffes afsted kommer, at alt kan samles i en IdP eller om der skal være to IdP løsninger for at fastholde de økonomisk favorable licensvilkår.

Hvis der er tid og handlerum, kan det evt. undersøges, om der er andre tolkningsmuligheder i de aftaler, der er med Microsoft, når man vurderer dels en AD løsning og en lokal IdP løsning. Det vil naturligvis være billigst for kommunen, hvis man kan nøjes med en IdP løsning uden at miste de favorable priser på uddannelseslicenser til skoleområdet. Ydermere vil et væsentligt punkt være det sikringsniveau man placere sig på, Lav eller Betydelig.

Det anbefales samlet set, at der etableres et målbillede med alle NSIS-krav, hvor de er kategoriseret som tekniske eller organisatoriske krav. Man kan overveje om der skal være to eller flere målbilleder, for hver IdP i kommunen, som skal overholde NSIS.

Ansatte i kommunerne skal på sikringsniveau betydelig

Det forventes som udgangspunkt, at alle ansatte, som skal have en medarbejdersignatur (undtagen borgerservice medarbejdere i RA-portalen, som skal være på Høj) skal have en lokal IdP bruger på sikringsniveau betydelig. Dette da forventningen er, at der ikke er fællesoffentlige løsninger, hvor kommunerne skal tilgå data og services, som kræver sikringsniveau Høj. Sikringsniveau Høj forventes også først understøttet af Digitaliseringsstyrelsen primo 2023.

Det er også på den baggrund, at der hos mange kommuner, Digitaliseringsstyrelsen og KL har været en tilgang til, at lokale IdP løsninger skal starte på sikringsniveau Betydelig. Men det er ikke utænkeligt, at som tiden går og føderationen vokser, vil der komme løsninger og services til, som vil kræve sikringsniveau Høj. Til den tid vil kommunerne have oparbejdet rutiner og erfaring både i forhold til drift og compliance, som gør det til en mindre krævende opgave at gå til sikringsniveau Høj i en lokal IdP løsning.

Skulle der mod forventning være nye fællesoffentlige løsninger, som kræver sikringsniveau Høj, vil kommunerne i perioden oktober 2022 frem til og med primo 2023 ikke kunne benytte disse fælles-offentlige løsninger. Kommunerne forventes i overgangsperiode for eksisterende fællesoffentlige løsninger at kunne anvende nuværende medarbejdersignatur uagtet krav til sikringsniveau indtil den nuværende medarbejdersignatur lukkes.

Vikar problematik og oprettelse i en IdP med tilhørende rettighedsstyring under NSIS

Håndtering af vikarer forventes at kunne være en potentiel udfordring. Dette kan være en af de opgaver, der gør det vigtigt, at have en manuel indrulleringsoption i valg af lokal IdP løsning.

Mange vikarer kender man ikke i kommunen, før de møder op til en indkaldt vagt. Når en vikar skal starte en nattevagt, hvordan skal plejehjemmet så sikre en korrekt indrullering og oprettelse i det

lokale IdP? Dette for, at vikaren med det samme kan starte med at arbejde og tilgå oplysninger i eks. FMK og tilsvarende systemer.

Ydermere kan opgaven kompliceres, hvis vikaren ikke har mulighed for at lade sig indrullere digitalt. Så skal der være en uddannet og certificeret medarbejder på plejehjemmet, som kan foretage en NSIS-korrekt identifikation af vikaren, før der må ske oprettelse i den kommunale IdP.

Det stiller store krav til at gennemtænke hele processen omkring at indkalde vikarer indenfor eksempelvis sundhedspleje i kommunen, hvor det kræver en erhvervsbruger udstedt i kommunens lokale IdP. Når oprettelsen i den lokale IdP er på plads, skal en brugeradministrator kunne tilgå rettighedsstyringen og pege på den konkrete vikar i det lokale IdP og give korrekte rettigheder i FMK og tilsvarende fællesoffentlige løsninger, hvor en vikar skal have adgang.

Det anbefales, at kommunerne i god tid overvejer, hvilken betydning det har for samarbejdet med vikarer og vikarbureauer. Skal der opstilles særlige NSIS-krav ved udbud af vikarydelser for at sikre, at vikarer enten allerede er indrulleret eller skal der ske andre tiltag forud for en start på vagt?

For at undgå problematikken med vikarer, kan kommunen beslutte, at det kun er fastansatte, der må have adgang til eksempelvis FMK med deres erhvervsbruger. På den måde kan man organisatorisk arbejde uden om vikarudfordringen i den kommende lokale IdP løsning, men det kan naturligvis være uhensigtsmæssigt i dagligdagen.

Del konklusion – Lokal IdP

NSIS-arbejdsområdet omkring lokal IdP er absolut det mest komplekse arbejdsområde. Ved første øjekast vil det formentligt blive håndteret ud fra et teknisk synspunkt, men dette er ikke nok. Det forretningsmæssige og organisatoriske behov skal medtænkes i forhold til, hvordan NSIS-kontrollerne efterleves.

Det anbefales, at kommunen orienterer sig i denne rapport med tjeklister, overvejelser og anbefalinger i forhold til det arbejde, der er igangsat i kommunen vedr. lokal IdP.

Det forventes, at hovedparten af alle kommuner skal anvende to eller tre IdP løsninger. Den ene IdP er den Nets leverer i RA-portalen til de ansatte i borgerservice. Derudover skal der til de øvrige ansatte i kommunen, som skal have en erhvervsbruger, være en IdP løsning til dem på minimum niveau Betydelig. Derudover kan der være kommuner, som vælger at videreføre en selvstændig IdP løsning til skoleområdet.

Hvis der ikke før udvikling/indkøb sikres korrekt organisatorisk understøttelse af NSIS-krav, vil en mangelfuld teknisk løsning forventes at kunne øge de organisatoriske omkostninger betragteligt.

Omkostningerne kan eksempelvis komme til udtryk ved, at der skal indkøbes tillægssystemer til at favne manglende NSIS-understøttelse af organisationens opgaver. Her tænkes særligt på, hvis der skal ske manuel indrullering i en IdP løsning.

Revisionserklæringer der skal udarbejdes i 2022

Kommuner, der vælger at købe eller selv bygge en lokal IdP, skal NSIS-anmelde deres lokale IdP-løsning til Digitaliseringsstyrelsen når den tilsluttes NemLog-in3. Disse kommuner skal i 2022 have udarbejdet en revisionserklæring pr. IdP løsning.

Kommuner bør allerede nu kontakte deres revisor for at få tilrettelagt en proces og få afklaret dels pris men også omfang af erklæringsarbejdet. Kommunen kan forvente en ikke uvæsentligt egen arbejdsindsats forbundet med udarbejdelsen af erklæringen og selve modningen af de arbejdsgange og dokumentationskrav, der skal opfyldes.

Kommunen skal herefter være forberedt på at få udarbejdet nye revisionserklæringer hvert år.

KL har indledt en dialog med revisorerne (FSR) og vil melde nærmere ud om dette i takt med, at det kan bidrage til den enkelte kommunes situation.

I dialogen med den udpegede revisor er det vigtigt at være opmærksom på, hvilken rolle det nuværende directory skal have i den samlede IdP-løsning. Valget kan udvide revisionserklæringen fra alene at favne den lokale IdP løsning, der er etableret, til også at favne hele brugerstyringen i kommunen. Det kan udvide det organisatoriske og tekniske scope fra et delelement af de ansatte til alle ansatte i kommunen.

Hvis man har flere IdP løsninger i kommunen, som skal være NSIS-compliant, så skal det afklares, om Digitaliseringsstyrelsen vil acceptere en samlet revisionserklæring, der dækker flere IdP-løsninger, som er indkøbt eller bygget til formålet.

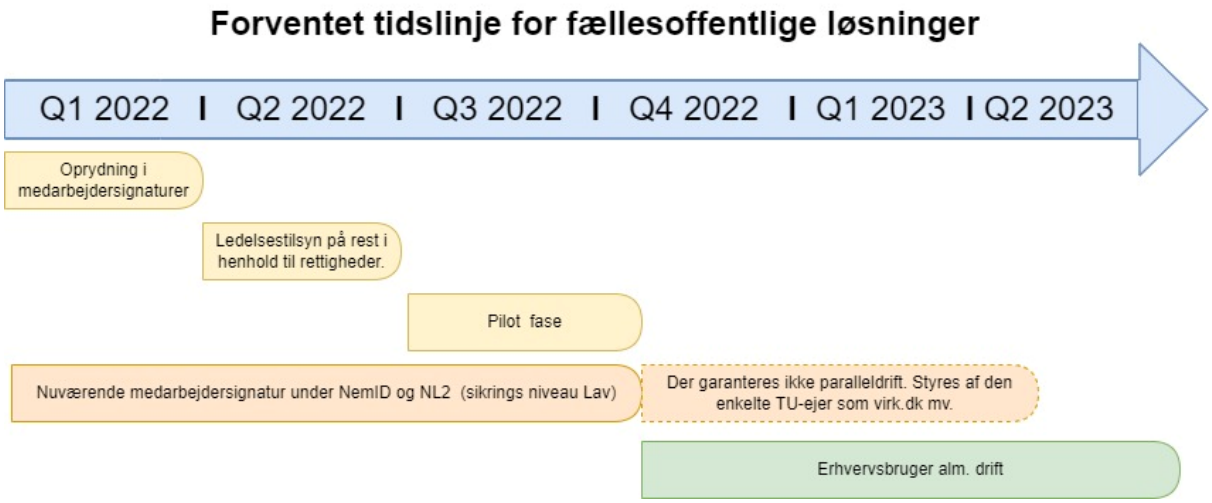
Fællesoffentlige løsninger og ekstern brugerstyring – spor 3

Dette NSIS-arbejdsområde ses ikke som komplekst ej heller som et teknisk krævende arbejde. Her er tale om, at kommunen skal omlægge de medarbejdere, der har en medarbejdersignatur med tilknyttede rettigheder i eks. virk.dk til, at de har samme rettigheder med den nye erhvervsbruger under MitID i samme virk.dk.

Nedenfor beskrives scenarie A og scenarie B. Det anbefales, at det rent teknisk sikres at man følger scenarie A. Dermed sikres en automatisk konvertering af rettigheder for alle kommunens brugere, der skal have en erhvervsbruger.

Det er endvidere vigtigt at bemærke, at alle brugere bør være oprettet og klar til brug dag et, når NL3 åbner for tilslutning af lokale IdP løsninger i produktion.

Nedenfor er tidsplanen, som det anbefales at følge baseret på den pt forventede tidsplan fra Digitaliseringsstyrelsen. Planen beskriver kun opgaver i regi af det tidligere nævnte spor 1.



Scenarie A)

NemLog-in3 tilbyder kommunerne at overflytte deres brugere fra medarbejdersignatur til MitID Erhvervsbruger, hvor hver bruger bl.a. beholder deres RID og evt. tildelte rettigheder i NemLog-in Brugerrettighedsstyring.

Via IdM API kan kommunen synkronisere disse brugere med deres eget lokale brugerkatalog og berige den centrale konto med det lokale brugerID – derved etableres link mellem central brugerkonto og lokal brugerkonto.

Der vil ske en automatisk omlægning af rettighederne i NL3 fra den gamle medarbejdersignatur til den nye erhvervsbruger i NL3, hvis kommunen sikrer, at RID nummer fra den gamle medarbejdersignatur påføres den nye erhvervsbruger i det lokale IdP

Dermed sikres en automatisk omlægning af rettighederne for kommunens brugere. I det omfang RID nummer ikke tages med, skal der ske en manuel omlægning, som beskrevet i scenarie B. Forventningen er dog at alle benytter sig af scenarie A hvorfor der ikke bliver brug for scenarie B.

Der ses følgende opgaver i scenarie A.

1) Ledelsestilsyn med oprydning i etablerede medarbejdersignaturer

   Kommunen anbefales at rydde op i de medarbejdersignaturer, der er oprettet, og sikre inaktive medarbejdersignaturer bliver lukket. Dette anbefales at ske i 1. kvartal.

2) Sikre RID nummer pr. bruger fra medarbejdersignatur så de er klar til oprettelse på den nye erhvervsbruger.

Scenarie B)

Overordnet er der disse opgaver:

1) Ledelsestilsyn med oprydning i etablerede medarbejdersignaturer

2) Kommunen anbefales at rydde op i de medarbejdersignaturer, der er oprettet, og sikre inaktive medarbejdersignaturer bliver lukket. Dette anbefales at ske i 1. kvartal. Identifikation af de fælles offentlige løsninger kommunen anvender

3) Identifikation af de ansatte i disse fællesoffentlige løsninger og dokumentation af deres rettigheder, evt. udfører ledelsestilsyn på disse også.

   I 2. kvartal 2022 bør der gennemføres ledelsestilsyn på de tilbageværende medarbejdersignaturer, for at sikre alle står med de rigtige rettigheder i forhold til deres arbejdsopgaver. Her menes de rettigheder, som medarbejderne har i fællesoffentlige løsninger som FMK m.fl., der blev identificeret under punkt 2. En vigtig opgave i arbejdet er også at identificere hvilke fællesoffentlige løsninger de enkelte medarbejdere kan tilgå.

4) Som med ny bruger, tilknytte en ansat til en fællesoffentlig løsning.

   4. kvartal 2022 starter oprettelsen af de nye erhvervsbrugere under MitID for de ansatte med en medarbejdersignatur.

5) Som med ny bruger, tilknytte rettigheder i den fælles offentlige løsning

Bilag 1 – Fællesoffentlige løsninger

Liste nedenfor indeholder fællesoffentlige løsninger, som kommuner i dag formodes at anvende for at kunne udføre deres opgaver i det daglige.

Listen bygger på kommunernes indmeldinger til KL og er ikke udtømmende. Den enkelte kommune skal derfor arbejde på at supplere listen med eventuelt yderligere fællesoffentlige løsninger, som anvendes i kommunen, altså fællesoffentlige løsninger, hvor de ansatte i kommunen skal logge på med deres medarbejdersignatur. Eksempelvis virk.dk, FMK m.v.

-

Arbejdsmarkedsportalen (STAR løsning)	Klageportalen på Nævnenes Hus
CPR/Folkeregister	Landbrugsindberetning.dk
CPR-selvbetjening	LER (Ledningsejerregistret)
CPRWeb	MoEva
CVR	NemId.nu
DIADEM	NemKonto
EASY	NemKonto Tilslutning
Easypark p-licens	Optagelse.dk
E-boks	Pilotafprøvning af PRO
Erklæring fra fodplejer/fodterapeut	Plandata
Fjern person fra min adresse	SEI (Sundhedsdatastyrelsens Elektroniske Indberetningssystem)
FMK - Fælles Medicinkort	Skat.dk
FK-admistrationsportal	Serviceplatformen
FUT Platform	STAR løsninger
Genoptræn.dk	Sundhed.dk
HjerteKomMidt	Sundhedstjenesten
Husdyrgodkendelse - Miljøstyrelsen	Tinglysning
InsuBiz	e-arkiv (sagsakter fra amterne) Miljøportalen
JobAG	Ejendomsregistreringsportalen
Jobnet.dk	Virk.dk
Almenstyringsdialog	Vitas
Indberetning af lån	Jobnet.dk
Tinglysningen	Minretsag.dk
bbr.dk	skat.dk
DPSD2	SOR-register
Kontakt Læge App	UTH
Nemkonto	BOSSINF-STB WEB

Bilag 2 – Ordforklaring og definitioner

Nedenfor nævnes nogle af de kerneelementer, det er vigtigt at kende for at læse og forstå rapporten og anbefalingerne korrekt.

Ord / definition	Forklaring
Medarbejdersignatur	Den nuværende medarbejdersignatur i NL2 løsningen.
Erhvervsbruger	Den nye kommende erhvervsbruger (MitID Erhverv) som fra den lokale IdP skal udstedes til de ansatte i kommunen. I første version kaldet erhvervssignatur.
NL2	Nemlog-in2 er den nuværende infrastruktur, der skal udfases og som indeholder NemID og medarbejdersignatur.
NL3	NemLog-in3 er den kommende infrastruktur, som skal afløse NL2 og som introducerer MitID til borgere og den nye MitID Erhverv erhvervsbruger til medarbejdere.
Manuel indrullering	Betyder at man i kommunen ønsker at identificere sine medarbejdere ved hjælp af fysiske dokumenter, som man gør i Borgerservice når en borger møder op og skal have udstedt MitID. Det vil sige ved hjælp af pas, kørekort mv.
Digital indrullering	Det betyder, at man indrullerer en medarbejder ved hjælp af det personlige NemID eller MitID.
NSIS-krav	Med udtrykket NSIS-krav tænkes på de kontrolområder og kontroller som Digitaliseringsstyrelsen opstiller som mindstekrav til den nye fællesoffentlige føderation NL3. Typerne af krav beskrives nærmere i afsnittet ” Introduktion til typer af NSIS-krav og tilgang til NSIS-krav ” i denne rapport.
Fællesoffentlige løsninger	Myndighedsløsninger som kommunerne skal benytte for at kunne løse deres opgaver. Eksempler på sådanne løsninger er virk.dk og FMK. Se bilag 1 for flere eksempler.
Compliance	Cmpliance betyder “overholdelse af regler, efterlevelse af retningslinjer” og benyttes som betegnelse for den eller processer, hvor en virksomhed forsøger at leve op til gældende krav og anbefalinger.
Digitaliseringsstyrelsens kontrolark til revisionserklæring	https://digst.dk/media/20289/bilag-a-skema-for-nsis-201-anmeldelse.xlsx Linket ovenfor henviser til Digitaliseringsstyrelsens anmeldelsesskema, som skal udfyldes ved anmeldelse af en lokal IdP til Digitaliseringsstyrelsen. Dokumentet skal udfyldes af både kommunen og revisor.

Delrapport 1 som KL udgav i april 2021	Link direkte til delrapport 1: https://videncenter.kl.dk/viden-og-vaerktoejer/informationssikkerhed-og-gdpr/nsis-national-standard-for-identiteters-sikringsniveauer/ Delrapport 1 som KL udgav i april 2021
Digitaliseringsstyrelsens dokument National Standard for Identiteters Sikringsniveauer (NSIS)	National Standard for Identiteters Sikringsniveauer (NSIS) - version 2.0.1a (digst.dk) I dette dokument er der en beskrivelse af NSIS-kontrollerne i kapitel 3.
NSIS-kontrol	Digitaliseringsstyrelsen omtaler selv kravene i NSIS-standarden som kontrolmål, men med kendt terminologi fra ISO27001 standarden kan de tilsvarende opfattes som kontroller. Fremadrettet vil kontroller og kontrolmål begrebsmæssigt kaldes foranstaltninger. Både i regi af NSIS men også helt generelt når der tales om informationssikkerhed. Begrebet foranstaltning kommer fra den nyeste ISO27002 vejledning, og vil også fremadrettet blive anvendt i ISO27001.
NSIS-ramme	Med udtrykket NSIS-ramme tænkes alle de NSIS kontrolmål som Digitaliseringsstyrelsen har stillet krav om, der skal opfyldes i kommunens valgte lokale IdP. Bemærk at det er kommunens målbillede, der på baggrund af primært de organisatoriske krav, rammesætter hvilke NSIS-kontrolmål, der kan udelades. Det vil sige at en kommune ikke nødvendigvis skal følge alle kontroller i forbindelse med etableringen af en Lokal IdP.
Målbillede	Med målbilledet menes at kommunen skal forholde sig til hvilke NSIS-kontroller, som afspejler de tekniske og særligt de organisatoriske behov i kommunen. Målbilledet skal afspejle hvad kommunen har besluttet i forhold til de tekniske, manuelle og fleksible kontroller. Herunder hvilke kontroller som ikke er relevante på baggrund af den organisatoriske tilgang, der er besluttet. Eks. om der er manuel eller ikke er manuel indrullering med i løsningen.

Bilag 3 – Ændringslog

I dette bilag fremgår de tilpasninger der er sket siden første udgivelse af version 1.00.

Side	Ændring
Alle	Der er gennemført en ændring af sprogbruget fra erhvervssignatur til erhvervsbruger.
Side 5 og 7 – Spor 3 opdateret med præciseringen.	Det er blevet uddybet, at der ikke blot er en webservice til omlægning af en medarbejdersignatur til en erhvervsbruger, men at kommunerne via IdP har mulighed for at registrere gammel RID nummer på ny erhvervsbruger. Herfra sker der i NL3 en automatisk omlægning af rettighederne. Det er meget positivt og en klar lettelse for kommunerne.
Side 8.	Det er præciseret, at kommunens egen revisionserklæring, ikke må være ældre end 90 dage, når en kommune anmelder en lokal NSIS IdP. Digitaliseringsstyrelsen accepterer indtil 12 måneder bagud fra leverandørerne, hvis de indgår i kommunens erklæring.
Side 9.	Det er præciseret, at der kun er krav om NSIS på de systemer, man lader indgå i NL3. Øvrige systemer, er ikke forpligtiget.
Side 13 og tidsplan generelt.	Digitaliseringsstyrelsen har præciseret at der ikke findes en overgangsperiode på 6 måneder.
Digitalt vitterlighedsvidne	Der findes endnu ikke et afprøvet produkt på markedet, derfor skrives det ud af rapporten. Emnet kan evt. indgå i erfa netværket som et emne der skal undersøges nærmere.