Spørgsmål	Svar fra KL	Dialog fra deltagerne
Hvordan tænker I så at holde os orienteret omkring hvor/hvornår der er/kommer opdateringer?	Vi deler materialer og opdateringer på KL og KOMBIT's videncenter, hvor rapporterne ligger.	
Er den nemme formulering af TU-løsninger, at det er løsninger der "kalder" NemLog-in?	Så simpelt er det ikke. Vi henviser til præciseringen af TU-løsninger som beskrevet i delrapport 1. Derudover er det vigtigt at have for øje, hvilke der er forpligtiget at tilslutte og hvilke man beslutter at tilslutte frivilligt. I det nuværende arbejde forholder vi os kun til NL3.	En TU-løsning er vel en hver løsning, som anvender NSIS LoA sikringsniveauer. De kan være fødereret med Nem-login men kan også være fødereret med en anden broker (f.eks. Context handler eller STil's Unilogin broker). En TU-løsning behøver derfor ikke nødvendigvis at forudsætte en MitID Erhvervsidentitet (men blot et NSIS LoA sikringsniveau). Derfor giver præciseringen med at anvende begrebet "Erhvervsbruger" også god mening.
Hvornår er dag 1?	24. oktober 2022.	Golive for tilslutning af Lokal IdP er d. 24/10-22 jvf tidsplan nederst på denne side Lanceringsdatoer for NemLog-in (digst.dk)
Jf. digitaliseringsstyrelsens udmelding om overgangsperiode, hvornår er skæringsdatoen så helt præcist?	24. oktober 2022.	
Skal alle relevante medarbejdere være indrulleret til skæringsdatoen så?	Ja, alle medarbejdere som i dag har en medarbejdersignatur skal være indrulleret i det lokale IdP den 24. oktober, hvis kommunen skal være 100% sikker på, at man ikke står i en situation, hvor der ikke er adgang til en TU-løsning.	

HVORDAN ved vi, hvornår en portal/fællesoffentlige løsninger overgår til den nye metode	KL følger udviklingen og melder ud i takt med at viden opstår.	
Er der et sted, hvor man kan få et overblik over, hvornår løsningerne skifter?	Ikke på nuværende tidspunkt.	
hjælper i med et overblik over mest brugte løsninger ift hvornår de skifter?	Se ovenfor.	
Vedr. konvertering af medarbejdere - hvem gør det og fra hvornår kan det gøres?	På webinar var vi kort inde på hvordan det praktisk kommer til at ske. Dette beskrives også yderligere i den opdaterede Delrapport 2 version 1.10.	
Hvem har mandat til at kræve/beslutte at en IT-Løsning fordre sikringsniveau >Betydelig<?	Det har tjenesteudbyderen.	
Hvilket ansvar har så Data-ansvarlig og hvilket ansvar har Data-behandler?	Som udgangspunkt bør det være den dataansvarlige, som godkender risikovurdering og sikringsniveau, der skal til for at tilgå data. Uagtet at det måske er databehandler som ejer og drifter en løsning.	
Så det er udelukkende leverandøren af løsningen som har det ansvar?	Det er tjenesteudbyderen/myndigheden, der har ansvaret	
Fx. KMD leverer løsningen "KMD-NEXUS" - Hvem har ansvaret her?	KL kontakter KMD	
Men det er jo vigtigt at vi ved hvem der i sidste ende "bestemmer". Skal vi som kommune kræve at fx. KMD løsninger retter ind til NSIS eller skal vi som kommuner bare afvente at KMD på eget initiativ tager NSIS ind i løsningen	KL kontakter KMD. Desuden pågår der et arbejde, hvor fælles kommunale løsninger risikovurderes af enkelte kommuner på	KMD er jo blot som eksempel - Dette vil jo være aktuelt for alle de leverandører som leverer løsninger til den offentlige sektor og generelt der hvor NSIS bringes i spil.

	alle 98 kommuners vegne. Arbejdet koordineres af KL.	
Dejligt at KL gerne vil hjælpe, men hvordan vil KL faktisk løse at man undgår at blive lukket ude? når man er lukket ude kan man jo ikke rulle tilbage, eller kan man?	KL kan ikke forhindre, at en tjenesteudbyder lukker af for brugere med "for lavt" sikkerhedsniveau	
Det giver rigtig god mening hvis KL vil stå for at levere et overblik frem for at vi henvender os til virk.dk FKM osv 98 gange	KL er enig. Overblikket findes dog ikke pt. og det bliver næppe nogensinde komplet.	
Hvilken app er der tale om i forhold til Fælles offentlig IdP?		
Hvis en af de store løsninger, som fx FMK, kræver niveau HØJ - giver det så anledning til at se på de tre søjler på anden vis?	Vi forventer niveau betydelig	
Vi har en udfordring med at finde ud af hvem der kan få MitID. Kan en svensk borger med CPR nr fra SKAT fx få MitID? Er det noget der beskrives i rapporten?	Nej, det er det ikke	
Digital indrullering, er det at bruge personligt MitID? Det er jo noget vi ikke kan "tvinge" medarbejdere til, så dermed er Fælles offentligt IdP udelukket?	Korrekt, hvis man ikke kan undvære manuel indrullering, så kan man som kommune ikke anvende den fælles offentlige IdP.	
er der kommet en løsning på personer med fremmed pas eller udenlandsk statsborgerskab	Her skal vi henvise til Borgerserviceområdet som ikke indgår i arbejdet.	Det afhænger vel reelt også af statsborgerskab - Dette kan jo i dag godt være 2 delt og dermed dække flere lande.

	Vi tænker, at der må være kommet instrukser til kommunerne fra Nets på vegne af Digitaliseringsstyrelsen på, hvem og hvad der skal til for at kunne udstede et MitID.	
Der er jo ikke så mange IDP løsninger på markedet. Kan I sige lidt om hvor de er placeret i matricen slidet? Eks. Signaturgruppens løsning og Digital Identitys løsning	Nej.	
Vi har også medarbejdere, der bor i Tyskland og ikke har NemID/MItID. Så har også brug for at de kan identificere sig manuelt. Kan det ikke gøres med udenlandsk pas?	Der kendes eksempler på tyskere som har NemID i dag og dansk CPR, selv om de bor i Tyskland. Men vi hverken kender ikke forudsætningerne for at de fik det, lige som vi heller ikke kender forudsætningerne for dem, der ikke har det i jeres eksempel. Det anbefales derfor at undersøge nærmere ude i kommunen, hvad der forhindre de ansatte i at få NemID. siden andre kan.	
Hvorfor/hvordan kommer vitterlighedsvidner ind? >S. 16 i rapporten<. Dette er helt ukendt hos vores leverandør af NSIS-løsning og hos dennes revision.	Kort fortalt kigges der i retning af det, der sker i borgerservice og de procedurer, der er her for anvendelse af vitterlighedsvidner ved udstedelse af MitID til en borger, som ikke kan identificere sig. Det er denne beskrevne	

	proces, der skal kigges på, om man kan digitalisere. Da der imidlertid ikke er noget kendt løsning tilgængelig pt., har vi valgt at fjerne det fra delrapport 2.	
Der er ikke udarbejdet risikovurdering endnu? (ifm. snak om 2 IDP'er)	Vi har ikke kendskab til, hvorvidt der er udarbejdet risikovurderinger ifm. vurdering af en eller flere IDP'er	
Hvad er KLs holdning til, hvis kommunen IKKE tilbyder manuel indrullering og man ansætter en medarbejder, som ikke kan få NemID/MitID - og som skal arbejde med opgaver, som kræver adgang til TU-løsninger? Må man undlade at ansætte dem eller må man afskedige dem?	Her må kommunens egne HR-jurister inddrages. Kontakt eventuelt KLs juridiske afdeling.	
Alle meldinger fra STIL indtil videre har da ellers været at vi skal forvente betydelig i forhold til UNV delen. Dette også for at man kan få adgang til sikker fildeling på Aula osv.	Vi arbejder i projektet ikke med STIL og deres tilgang til området. Vi forholder os kun til at der muligvis skal etableres 2 IdP løsninger i kommunen. En til det administrative personale og muligvis en til skoleområdet. Her er vores anbefaling at der opsættes et målbillede for behov og ønsker. Her skal indgå evt. krav fra STIL som skal adresseres / løftes i målbilledet.	

Det springende punkt bliver om Aula overgår til at anvende NSIS sikringsniveauer, hvilket mig bekendt fortsat er uafklaret. Hvis Aula overgår til NSIS at anvende NSIS sikringsnivauer, så skal IdP'en på B&U området anmeldes på Betydelig niveau, så medarbejderne kan logge på "sikker fil" området i Aula.	Korrekt, her afventes en AULA beslutning.	børn er jo defacto høj risiko og fortjener særlig sikring i realtion til databeskyttelse, så den lave risiko går nok ikke helt
Har I været i dialog med nogle fagsystemleverandører omkring denne problemstilling? - Hvis ja - Hvilke?	Vi har ikke talt med leverandører om vikarer	
Hvorfor ikke inddrage leverandører til en så vigtig problemstilling i arbejdet med rapporten? Både leverandører af vikarer og dem som leverer løsninger der anvendes til opgaverne	KL har ikke kendskab til hvorfra kommunerne henter vikarer	
Har det ikke betydning for hvilken adgang vikaren skal have? AT de systemer som vikaren skal have adgang til alle er på niveau lav?	Det afhænger af systemerne og login metoden	
Hvor står kravet omkring 24/7 support?	Som det allerede blev skrevet ind i chatten af deltagerne, så fremgår det af NSIS krav 3.2.3.6. Tilgangen er, at har man manuel indrullering, så har man formentligt også en manuel support, der skal være tilgængelig. Med ren digital indrullering kan man udstille denne support digitalt og dermed slippe for manuel support.	Krav om 24/7 support står i krav 3.2.3-6 pkt. 3.2.3.6 er for betydelig nej, kravet om 24/7 gælder muligheden for spærring/suspendering Kravet 3.2.3-6< indeholder ikke krav om 24/4 support. Det kræver blot at "Suspenderings- og spærrefunktionen skal være til rådighed døgnet rundt og have en høj grad af tilgængelig" = At brugeren skal altid selv kunne låse/åbne sin konto såfremt denne er spærret. Så hvis de elektronisk selv kan bestille en "nul-stilling" af fx passsord er kravet

	Det skal dokumenteres at alle support scenarier er løftet digitalt. Brug målbilledet til denne nærmere afklaring af hvordan i løser kravet.	opfyldt. Vi skal altså ikke stille telefonsupport eller andet til rådighed. Jo, hvis I accepter manuel verifikation. Ellers kan I nøjes med selvbetjeningsportalen.
Uanset løsning kan vi vel altid komme ud i at skulle indrullere "nægterne" manuelt?	Det afgør den enkelte kommune	Vores tanke er, at det er vores Borgerservice skulle indrullere medarbejdere manuelt - vi har slet ikke tænkt i, at det kunne decentraliseres. Det kræver jo, at dem, der håndterer opgaven, er uddannet i det
Manuelt oprettede medarbejdere, kan vel godt gå ind i den digitale løsning efterfølgende, for at nulstille, vælge nyt identifikationsmiddel, mv. Så er 24/7 support-kravet ikke kun relevant for INDRULLERING?	Når vi snakker manuel indrullering, så er det helt sikkert, der er et behov. Men afhængig af om en bruger er låst/spærret eller suspenderet, så skal man reelt kunne indrullere igen forfra manuelt. Så de facto har man en 24/7 support, for en bruger kan få brug for denne hjælp midt om natten, mens de er på arbejde. Der kan kun afhjælpes digitalt i nogen af situationerne.	
"....nuværende NemID" betyder det "personligt NemID"?	Ja, NemID er det private NemID man har som privat person.	
En medarbejder der ønsker den manuelle indrullering får skiftet password af f.eks. IT skal vel igennem samme proces for at opnå samme NSIS niveau?		IT kan ikke skifte password fremadrettet - det må vi ikke!

		vi kan heller ikke
hvilken lovhjemmel har digitale vitterlighedsvidner? der er jo konkrete habilitets krav til vitterlighedsvidner som måske er lidt udfordret digitalt?	Det skal følge den proces man som kommune kender i borgerservice i RA-portalen.	
Vi påtænker, at medarbejderne også ud over indrullering skal anvende deres MitID som identifikationsmiddel. Er det et problem?	Medarbejder kan bruge deres private MitID så meget de vil i arbejdsøje med. Det kalder Digitaliseringsstyrelsen det dobbelte frivillighedsprincip. I NSIS fremgår der også en række krav man skal overholde, hvis man ønsker dette. Vores anbefaling er dog at fokusere på at den enkelte medarbejder får en erhvervsbruger i det lokale IdP. Det betyder, at den eneste gang en medarbejder skal bruge deres personlige NemID eller MitID er, når de lader sig indrullere første gang. Det vil sige, at i beder jeres medarbejder identificere sig med deres digitale "ID-kort" på samme måde, som i kan bede dem identificere sig med deres fysiske ID-kort som pas eller kørekort.	Så skal det vel op på direktionsniveau, at det er det i kræver af medarbejderen. Brug af MitID (privat i hverdagen) til at steppe op.... det er ikke en god ide Man kan godt bruge sin private NemID - det må blot ikke være den eneste mulighed. Som jeg husker afgørelsen fra Datatilsynet.
Er der lovhjemmel til at kræve brug af privat NemID/MitID? Jeg har ikke kunne finde sådan hjemmel nogetsteds. Dermed kan man vel ikke komme udenom at tilbyde manuel indrullering?	Der er ikke lovhjemmel til at kræve brug af privat NemID/MitID	Som jeg forstår det, så skal medarbejderen selv vælge, hvilke identifikationsmidler de ønsker at anvende i hverdagen. Og som jeg forstår det kan NemID/MitID være en

		valgmulighed på linie med hardware nøgler, 2Faktor-apps, mv. Så er det jo op til medarbejderen selv at beslutte om de ønsker at…
		ENIG, men vi tvinger dem ikke til at bruge det…
Er der lovhjemmel til at kræve brug af privat NemID/MitID? Jeg har ikke kunne finde sådan hjemmel nogetsteds. Dermed kan man vel ikke komme udenom at tilbyde manuel indrullering (uanset hvad lokal ledelse eller andre så har af holdninger)?	Se ovenfor.	Lasse, tænker på at det omvendte spørgsmål er lige så relevant. Er der lovhjemmel der siger at man ikke må kræve identifikation med personligt MitID, når man skal have udleveret/aktiveret et andet loginmiddel
		Man kan som arbejdsgiver godt stille det krav….altså anvendelse af privat NemID/MitID
		NemID/MitID - få nu en ledelsesmæssig beslutning ud fra indblik i de tekniske og revisionsmæssige krav om, at vi alene arbejder med digital identifikation. Løft en pædagogisk drøftelse i MED-organisationen. Lad det herefter blive en ledelse og medarbejder drøftelse, hvilke opgaver vedkommende medarbejder så ikke skal løse, da vedkommende ikke får adgang til data klassificeret som Betydelig. PS - det tager lang tid, men det gør en manuel løsning også, så de fleste kommuner vil være presset iht. den fremlagte tidsplan
Hvornår planlægges opdatering af rapporten, netværk mv. ? (vi er jo i gang)	Rapporten er opdateret og findes samme sted som dette notat. Netværk er ikke endeligt planlagt.	

Rapporten side 20 - Hvis man har flere IdP løsninger..... Hvordan afklarer vi i praksis som kommune om Digitaliseringsstyrelsen vil acceptere en samlet revionserklæring	KL går i dialog med Digitaliseringsstyrelsen for at afklare de nærmere muligheder.	Ifølge digitaliseringsstyrelsen kan man godt anmelde 2 IdP'er på samme anmeldelse og med én revistionserklæring.
	Se tidligere svar.	Jeg har forstået det sådan, at hvis man har medarbejdere delt op i to forskellige AD'er - så er der behov for 2 revisionserklæringer.