Vangsaa Consult
Sct. Hansgade 9
4100 Ringsted

Telefon: 7199 5206
E-mail: Info@VangsaaConsult.dk
WWW: VangsaaConsult.dk

Kommuner som tjenesteudbydere og nye krav fra NSIS.

Version:	1.00
Udgivet:	25. marts 2021
Udgiver:	Vangsaa Consult ApS, på bestilling af KL.

Indhold

KL's forord

Danmarks offentlige sektor udnytter i meget høj grad de digitale og teknologiske muligheder, både med de løsninger, der anvendes i den enkelte kommune og med de løsninger, der anvendes på tværs af myndigheder og borgere mv. Kommunerne er således i høj grad afhængig af sikre -forbundne enheder og systemer. Med stigende trusler og øget fokus på sikker håndtering af borgernes data, er sikkerheden i håndteringen af de mange forbundne kar helt central. Det stiller større og større krav til håndteringen af informations- og cybersikkerhed i kommunerne. Og dermed stiller det også voksende krav til måden, kommuner håndterer brugernes identiteter og adgang til løsningerne.

Det er således brugerstyringen og krav til denne, der er udgangspunktet for denne rapport. Brugerstyring er blevet et mere og mere kritisk element i it- og informationssikkerhed. Det opleves dagligt ift. sikkerhedsudfordringer og det ses tydeligt i, at der via direktiver og forordninger fra EU stilles større og større krav til lande og myndigheders håndtering af dette. Det indgår således i GDPR, i eIDAS og det ses i forlængelse af dette, som noget der er fokus på ved tilsyn med myndigheder mv. Senest set ved Rigsrevisionens behandling af ministeriers tilrettelæggelse af brugerstyring i offentlige tilskudsløsninger.

For at understøtte og sikre en sammenhængende og fælles tilgang til, hvordan man arbejder med brugeres identiteter på tværs af den offentlige sektor, har Digitaliseringsstyrelsen udviklet en national standard for identiteters sikringsniveau (NSIS). Den skal skabe rammerne for tillid til brugeres digitale identiteter og til de digitale id-tjenester, så myndigheder kan have tillid til identiteter, der er skabt hos andre myndigheder. Det er en væsentlig brik for fremtidens digitale samarbejde i den offentlige sektor.

Standarden er og skal fremover fungere som referenceramme for kommuners (og øvrige myndigheders) tilrettelæggelse af arbejde med identitets-sikring og brugerstyring.

Det kommende MitID og Nemlog-in3 stiller således krav om overholdelse af NSIS, for at kommunen kan anvende disse og indgå i det kredsløb, der er omkring disse løsninger. Her bliver kravene lagt ind i lovgivningen og der er således frister for, hvornår kommunen skal leve op til NSIS-standarden ift. disse. Der er og har været mange spørgsmål om anvendelsen af standarden i den sammenhæng og hvad det konkret betyder for de kommunale systemer og hvad og hvordan kommunerne skal gribe denne opgave an. Det er baggrunden for denne delrapport 1og dermed også afgrænsningen ift, hvad der belyses i rapporten.

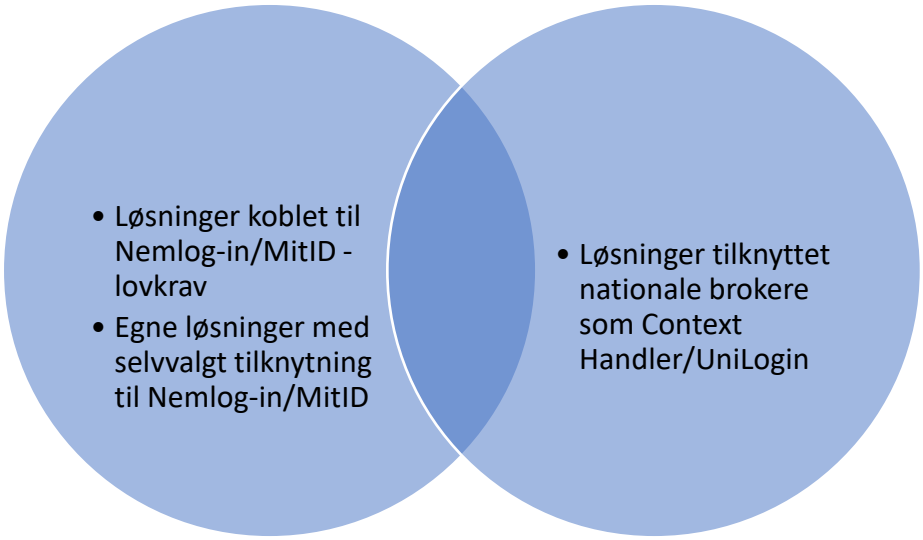
Da NSIS er den nationale standard for identiteters sikring, anvendes denne også i andre sammenhænge, hvor løsninger går på tværs af myndigheder og/eller er båret af internettet. Disse typer løsninger benævnes tjenesteudbyder løsninger (TU-løsninger), og er

kendetegnet ved at løsningen er tilgængelig for kommunens borgere via logon med NemID eller er tilgængelig for virksomheder via logon med medarbejdersignatur. NSIS anvendes også ift. nationale brokere, som f.eks. Context Handleren i KOMBIT og STILs UniLogin. Her stilles der således de samme krav til brugerstyringen i kommunerne som ved TU-løsninger.

Anvendelsen af standarden er en fornuftig og sikker måde til at sikre, at man lever op til en lang række af de krav, der i øvrigt er til håndtering af informations- og cybersikkerhed, f.eks. i forlængelse af GDPR.

De løsninger, som skal bruge NemLog-in3 på baggrund af loven, behandles i denne rapport som inspiration for den kommunale opgavetilrettelæggelse, når kommunen implementerer NSIS-standarden lokalt og i fællesskab.

Der er en række løsninger, der ikke bliver udbudt til andre brugere end medarbejdere i den enkelte kommune. Her kan det strategisk og praktisk være en fordel at opbygge brugerstyringen ud fra den samme grundlæggende referenceramme, som resten af systemlandskabet, men det er ikke et krav og derfor noget, den enkelte kommune skal tage stilling til efter egen vurdering af behov, risici, mulighed for praktisk tilrettelæggelse mv. Samlet betyder det, at den kommunale bruger- og rettighedsstyring møder krav om at leve op til NSIS, enten via lovkrav, via krav fra nationale brokere og tilknyttede systemer eller fra egne ønsker om en sammenhængende, professionaliseret identitets- og brugerstyring. Figuren illustrerer, hvordan løsninger, der er påvirket af NSIS, fordeler sig.



Denne rapport tager fat i opgaverne med at identificere de løsninger, kommunerne skal fastlægge sikringsniveauer for, for at løsningerne kan fungere også efter at MitID og den fremtidige NemLog-In3 træder i kraft med udgangen af 2021. For at støtte kommunerne bedst muligt i arbejdet faciliterer KL en række workshops i forlængelse af denne rapport,

hvor kommunerne i samarbejde afdækker de TU-løsninger, som flere kommuner anvender, og sammen fastlægger sikringsniveauet.

Rapporten indeholder ikke bud på kommunernes egne interne løsninger, der hverken bruger nuværende NemLog-in eller er tilknyttet andre nationale brokere end NemLog-in. For denne gruppe af løsninger indeholder rapporten en række tjeklister, der kan bruges som inspiration.
Kommunernes opgaver er de samme og i mange tilfælde anvendes de samme IT-løsninger på tværs af flere eller alle kommuner. Ligesom der også ofte arbejdes på tværs af løsninger indenfor eller mellem kommuner. Derfor er der behov for en fælles tilgang til håndteringen af NSIS, så muligheder for fortsat at kunne udveksle fleksibelt og smidigt fastholdes, og så hver enkelt kommune ikke nødvendigvis skal løfte hele opgaven selv. Når den kommunale brugerstyring og identitetssikring skal håndtere NSIS, kræver det således en fælles tilgang. Det gælder i den nødvendige dialog med it-leverandører. Og det gælder i dialogen med revisorerne. Samtidig rejser det en række naturlige spørgsmål om, hvad der skal til for at møde kravene til to faktorer ved login og til, hvordan og hvor længe faktorerne holder, før de timer ud. Det er spørgsmål, som der ikke findes entydige svar på i dag.

Denne rapport peger på håndtering af praktiske opgaver med at identificere hvilke borger- og virksomhedsrettede tjenester ift. NemLog-in3, kommunen skal stille krav om sikringsniveau til. Og den næste rapport i arbejdet - delrapport 2 - bliver rettet mod opgaver og udfordringer for tilrettelæggelse af IdP med videre.

Ledelsesresumé

KL's NSIS-projekt forsøger at samle Digitaliseringsstyrelsens forskellige udrulningsplaner i fire arbejdsområder. De fire arbejdsområder er, tjenesteudbyder løsninger, Borgerservice, lokal IdP og brugerstyring i fælles offentlige løsninger som virk.dk, FMK mv.
På tværs af de fire arbejdsområder arbejdes der særligt med fokus på National Standard for Identiteters Sikringsniveauer (NSIS) og standardens indvirkning på de fire arbejdsområder.
Rapporten har udpeget disse fire arbejdsområder da disse er afledt af omlægningen fra NemLog-in2 til den fremtidige NemLog-in3 broker.

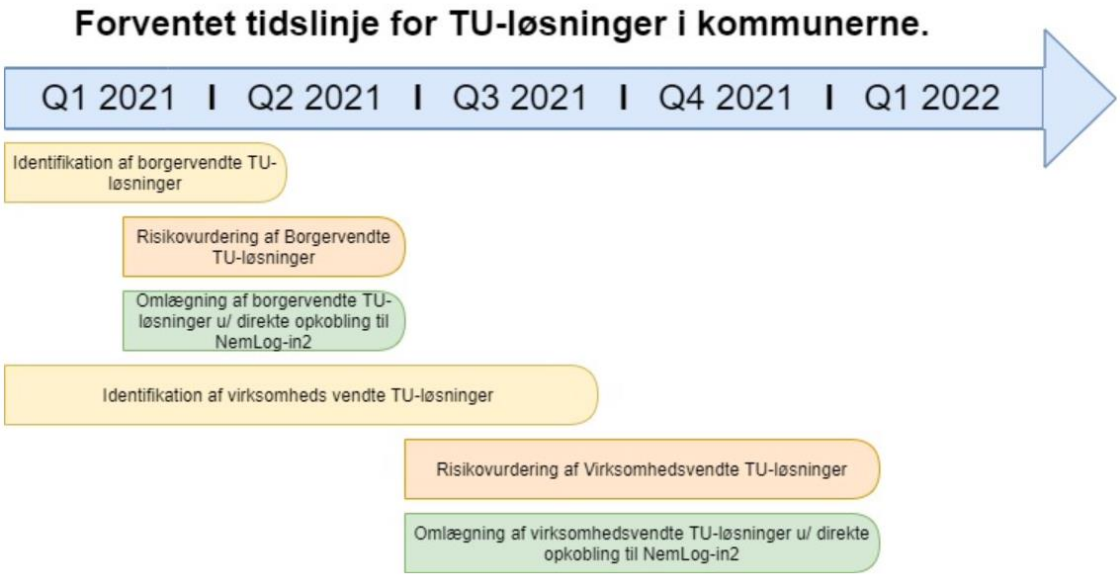
Denne delrapport 1 arbejder med og forholder sig kun til det ene arbejdsområde tjenesteudbyder løsninger (fremover benævnt TU-løsninger) hvor kommunerne har en aftale med Nets, på vegne af Digitaliseringsstyrelsen, om opkobling af en tjenesteudbyder løsning til den nuværende NemLog-in Broker.
Der kan være andre kommunale løsninger som tilsvarende skal arbejde med NSIS. KOMBIT har meldt sikringsniveauer ud for deres løsninger. Ligeledes forventes STIL at kommunikere direkte med kommunerne.
Disse løsninger er derfor ikke inkluderet i denne rapport.

Den næste rapport (delrapport 2) vil behandle de tre arbejdsområder, Borgerservice, lokal IdP og brugerstyring i fælles offentlige løsninger som virk.dk, FMK mv.
Se afsnittet delrapport 2 sidst i denne rapport vedr. indhold.

Delrapport 1 er udarbejdet på baggrund af data fra kommunerne selv og via løbende sparring med KL. Se bilag 1 for et hurtigt overblik af besvarelser fra kommunerne og bilag 2 for metodeindsamling.

Kommunerne har det formelle ansvar for at placere TU-løsningerne på det korrekte sikringsniveau. Vangsaa Consult forventer på baggrund af Digitaliseringsstyrelsens definitioner, at det højeste niveau på kommunalt plan, bliver sikringsniveau Betydelig. Herudover kan der være løsninger som kan indplaceres på sikringsniveau Lav.

Arbejdet med NSIS hænger tæt sammen med implementeringen af nyt MitID og NemLog-in3 og det vurderes at disse løsninger bliver dem, der reelt bliver de første til – i praksis – at introducere krav om NSIS-efterlevelse. Derfor er der en række deadlines, som arbejdet skal holdes indenfor. Nedenfor gengives meget kort en oversigt over deadlines kommunerne skal arbejde med.



På baggrund af analysen er der udarbejdet et afsnit med definitioner af TU-løsninger og typer, da det ikke ser ud til at være helt klart hvordan disse skal opfattes i forhold til NSIS-opgaven. Det forventes dog at det tekniske arbejde med TU-løsningerne ikke er en uoverskuelig opgave for kommunerne, da hovedparten af kommunernes TU-løsninger i forvejen har et teknisk setup, der kobler direkte op til den nuværende NemLog-in2 broker. Der findes dog TU-løsninger som kræver en del mere arbejde (i figuren ovenfor benævnt som TU-løsningen u/direkte opkobling til NemLogin2), men det vurderes ikke at være en stor del af de samlede TU-løsninger hos kommunerne. Dette gælder for TU-løsninger som ikke kobler direkte op på NemLog-in2 brokeren samt TU-løsninger hvor dokumenter kan signeres i dag.

For at støtte kommunerne bedst muligt i arbejdet anbefales det, at KL faciliterer afholdelse af en række workshops i forlængelse af denne rapport. Tilgangen med workshops er at kommunerne i samarbejde løfter risikovurdering og fastsættelse af TU-løsninger, som flere kommuner anvender.

Der vil være kommuner med egne individuelle løsninger som ikke kan håndteres i regi af de fælles workshops hos KL. Her skal de enkelte kommuner selv sikre at opgaverne identificeres og løses før ovennævnte deadlines.

Introduktion

Denne rapport er målrettet ansatte i kommunerne som skal arbejde med at forberede kommunen på omlægning til den nye fællesoffentlige føderation NemLog-in3 og herunder MitID, som fordrer efterlevelse af NSIS. Rapporten er tiltænkt at give programledere, projektledere samt projektdeltagere et indblik og overblik over de opgaver, der skal arbejdes med. Rapporten har i mindre grad fokus på en teknisk tilgang, men i højere grad en forretningsmæssig og organisatorisk tilgang til opgaverne.

NSIS stiller en række nye krav til kommunerne i forhold til organisationen og rent teknisk. Compliance dokumentation kommer til at fylde en del mere, end kommunerne er vant til. Teknisk set får NSIS betydning for den fremtidige opkobling og anvendelse af TU-løsninger i kommunerne.

Helt overordnet er NSIS-opgaven omkring TU-løsninger initialt, at de skal risikovurderes og indplaceres på det korrekte sikringsniveau. Samtidig skal der indgås TU-tilslutningsaftaler med Digitaliseringsstyrelsen (DIGST). Det er endnu ikke afklaret, hvordan TU-tilslutningsaftalerne indgås.

Den overordnede opgave er ens for alle kommuner, uanset TU-løsning, men der er dog variationer afhængig af hvordan kommunen har indkøbt eller etableret TU-løsningen.
Det forventes at hovedparten af alle TU-løsninger har et teknisk setup (NemLog-in2 og NemID), hvor det ”blot” handler om at udføre opdateringer i takt med, at de kommer fra Nets (Digitaliseringsstyrelsen) for at komme på NemLog-in3. Ved disse løsninger forventes heller ikke opgaver i overgangsfasen.
Der er kendskab til at nogle kommuner har TU-løsninger, som ikke følger den almindelig opsætning, og dermed kommer til at give en del ekstra opgaver. Derfor kommer Vangsaa Consult med anbefalinger senere i rapporten til, hvad kommunerne skal overveje, og undersøge, for at sikre der ikke glemmes noget i de få TU-løsninger, som kan have en mere kompleks opsætning. Konsekvensen ved ikke at identificere og afhjælpe disse udfordringer, kan være at borgere og andre ikke kan logge på de glemte TU-løsninger.

Udover NSIS-kravet om en risikovurdering og etablering af nye TU-tilslutningsaftaler med Digitaliseringsstyrelsen (DIGST), forventes der ikke de store opgaver i forbindelse med overgangsperioden for kommunernes TU-løsninger. DIGST har på nuværende tidspunkt (marts 2021) ikke præsenteret en revideret udgave af TU-tilslutningsaftalen.

Rapporten skal ses som en støtte til kommunernes arbejde omkring NSIS og TU-løsninger, men rapporten har også det formål at skabe en fælles forståelse for og tilgang til TU-

løsninger. Herunder at opstille en begrebsramme, som hjælper kommunerne med at kunne være fælles om arbejdet og dermed skabe synergi hos kommunerne i forhold til den samlede kommunale opgave. Kommunerne kan læse mere omkring de opgaver, der er til deres arbejde med og håndtering af TU-løsninger i rapporten. Derudover skal rapporten ses som en hjælp til tolkning og vejledning, samt forslag til fremgangsmåde for håndteringen af TU-løsninger.

Sikringsniveauer - TU-løsning

Nedenfor præsenteres Digitaliseringsstyrelsens beskrivelse af de tre sikringsniveauer for en TU-løsning.

Beslutningen om sikringsniveau for en TU-løsning træffes i den enkelte kommune på baggrund af de risikovurderinger, der udføres pr. TU-løsning. Vangsaa consult forventer ikke, at der findes kommunale TU-løsninger på kommunalt plan, som skal på sikringsniveau Høj. Dette baseres på definitionerne fra Digitaliseringsstyrelsen.

Nedenstående eksempler er fra Digitaliseringsstyrelsens vejledning til valg af NSIS Sikringsniveau for tjenesteudbydere Version 2.0.2:

- **Sikringsniveau Lav**

"En kommunal tjeneste til bestilling af ekstra skraldespande kan ud fra en risikovurdering komme frem til, at det er tilstrækkeligt, at brugerne er autentificeret på Sikringsniveau Lav. En bruger, som anvender et Elektronisk Identifikationsmiddel på dette niveau (fx baseret på brugernavn/kodeord), bør derfor få adgang."[1]

- **Sikringsniveau Betydelig**

"En tjeneste, som giver borgere adgang til egne sundhedsdata, kan ud fra en risikovurdering komme frem til, at det er nødvendigt, at brugerne er autentificeret på mindst Sikringsniveau Betydelig."

[1] Teknik og miljø i flere kommuner har igennem årene efterlyst at man med NemID kan nøjes med brugernavn og password. Med det fremtidige MitID åbnes der op for dette kommunale ønske omkring èn faktor login. Definitionen af sikringskravene for Lav, Betydelig og Høj er præciseret i NSIS krav 3.2.1., som uddybes og beskrives nærmere i Digitaliseringsstyrelsens vejledning til valg af NSIS Sikringsniveau for tjenesteudbydere

Her er brugernavn/kodeord ikke længere nok. Her skal der bruges 2 faktor tilgang som understøttes med NemID / MitID. Formålet er at identificere at den pågældende person, er den vedkommende siger, men også at vedkommende har ret til at bruge systemet på dette sikringsniveau.

- **Sikringsniveau Høj**

"En tjeneste, som giver sundhedsfaglige medarbejdere adgang til følsomme personoplysninger om et meget stort antal borgere, kan ud fra en risikovurdering komme frem til, at det er nødvendigt, at brugerne er autentificeret på Sikringsniveau Høj."

Hvad er en TU-løsning?

På baggrund af analysen, ses det nødvendigt at definere TU-løsningerne mere konkret, samt skabe en fælles forståelse af hvad de forskellige TU-løsninger indebærer. Nedenstående afsnit skal derfor hjælpe til en ensartet opfattelse, samt forståelse for hvad en TU-løsning er, samt beskrive de tre typer TU-løsninger, der defineres i dette projekt.

TU-løsning – definition

Dette afsnit er en gennemgang af typer af TU-løsninger, som kommunen skal arbejde med i forhold til eksisterende TU-løsninger.

IT-systemet opfattes som en TU-løsning, hvis det opfylder et af følgende kriterierne:

- IT-systemet skal være tilgængeligt for kommunens borgere via logon med NemID
- IT-systemet skal være tilgængeligt for virksomheder via logon med medarbejdersignatur.

Det betyder kort sagt, at en TU-løsning som regel er en digital selvbetjeningsløsning, hvor en borger/medarbejder i en virksomhed kan logge på med NemID/Medarbejdersignatur og derefter være selvbetjent hos kommunen.

Typer af TU-løsninger

Nedenfor vil de to typer af TU-løsninger blive gennemgået, samt præsenteret med eksempler på, hvordan de lever op til de to kriterier.

I dette afsnit er der forslag til hvordan TU-løsninger kan inddeles i forskellige typer. Denne tilgang er valgt, da der er varierende opgaver og opgaveomfang afhængig af hvilke TU-løsninger, den enkelte kommune har.
På de efterfølgende sider kommer rapporten ind på de to typer af TU-løsninger, hvor kommunen skal udarbejde eller godkende en risikovurdering. De to typer er listet med den, der er mest arbejde ved først og den sidste, hvor der er mindst arbejde.

- Egen TU-løsning
- TU-løsning, som flere kommuner anvender

I de efterfølgende afsnit, forklares og beskrives hvordan man skal forstå de to typer af TU-løsninger.

Hvad er en egen TU-løsning?

I denne kategori drejer det sig om TU-løsninger, hvor kommunen er den eneste, der anvender IT-systemet. Det kan både være TU-løsninger, der er udviklet af kommunen selv eller købt hos en ekstern leverandør. Der er ikke andre private eller offentlige kunder der anvender det pågældende IT-system hos leverandøren.

F.eks. har en kommune indberettet, at de har fået udviklet et IT-system som opfylder et kriterie for at være en TU-løsning; systemet er tilgængeligt for borgerne, der logger på med deres NemID og derigennem selv kan bestille parkeringstilladelser.

Her ses det at TU-løsningen opfylder betingelserne, da kommunen selv har udviklet systemet, det er tilgængeligt for borgerne, der kan betjene sig selv ved at logge på med NemID. Ingen andre end den pågældende kommune bruger dette system.

Hvad er en TU-løsning, som flere kommuner anvender?

TU-løsninger af denne type ses, når der er flere kommuner, der bruger samme IT-system. Ofte er det indkøbt i mindre grupper af kommuner, der er gået sammen, eller der er tale om en privat leverandør, som enkeltvis har solgt det til flere kommuner. Det behøver ikke kun være kommuner der anvender TU-løsningen, det kan også være private virksomheder, statslige eller regioner, der anvender den private leverandørs TU-løsning. Fællesnævneren er, at der skal være flere anvendere af samme system, for at der er tale om en fælles TU-løsning.

Tabulex er et eksempel på en TU-løsning, som flere kommuner anvender, da der er tale om en privat udbyder, hvor flere kommuner og private virksomheder har købt adgang til systemet. Her ses det, at systemet er tilgængeligt for borgere, der benytter NemID. I denne løsning har medarbejdere også adgang og skal logge på løsningen med medarbejder Signatur, således de kan betjene dem selv i systemet.

Aula er et andet eksempel på en TU-løsning som flere kommuner anvender. Aula lever op til kriterierne om at være en TU-løsning, da login foregår med bl.a. NemID og den er tilgængelig for borgere men også kommunens medarbejdere, hvor alle parter kan betjene sig selv.

Fællesoffentlig løsning (tidligere kaldet myndighedsløsning)

I analysen fremgår det at flere kommuner oplyser fællesoffentlige løsninger som værende kommunens egen eller en TU-løsning, som flere kommuner anvender. Dette er en misforståelse, og derfor følger en uddybning af, hvad en fællesoffentlig løsning er, og hvorfor det ikke er en TU-løsning, hvor kommunerne har ansvaret og opgaven med at udarbejde en NSIS-risikovurdering.

Et IT-system skal opfattes som en fællesoffentlig løsning, hvis det opfylder følgende kriterier:

- IT-systemet skal være tilgængeligt for kommunens ansatte
- IT-systemet tilbyder kommunen og dens ansatte, at udføre arbejde og services som kommunerne er forpligtiget på
- IT-systemet tilhører en anden myndighed eller offentlig organisation

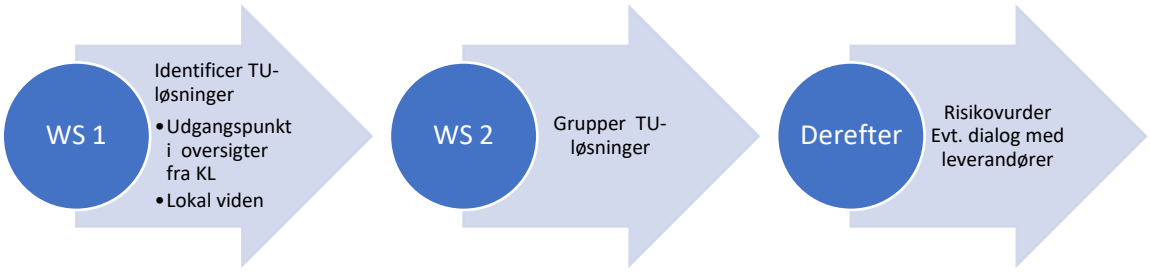
Fælles Medicinkort (FMK) er et eksempel på en fællesoffentlig løsning. Her er tale om et IT-system som ansatte i kommunen kan tilgå og anvende i deres daglige arbejde, men systemet ejes af Sundhedsdatastyrelsen. Selv om FMK er en TU-løsning, så er det ikke kommunens TU-løsning og dermed har kommunerne ingen opgaver i forhold disse løsninger.

Hvordan identificeres TU-løsningerne

Identifikation af TU-løsninger som flere kommuner anvender

Det anbefales at der afholdelses workshops med deltagelse af kommunale medarbejdere, hvor de fælles løsninger identificeres og risikovurderes. Der tages udgangspunkt i definitionerne for TU-løsninger i denne rapport, spørgeskema hvor den enkelte kommune har angivet deres TU-løsninger, oplysninger fra KITOS samt viden hos deltagerne.

Herefter kan en yderligere gruppering af TU løsninger ske pr. fagområde / pr. leverandør eller hvad der findes mest hensigtsmæssigt. Dette besluttes på workshoppen. Her er det vigtigt at fokusere på om løsningerne indeholder følsomme og/eller fortrolige data, da dette kriterie vil skulle bruges ifm. risikovurderingen.
Efterfølgende kan TU løsningerne indenfor de enkelte grupper risikovurderes.



Da det kun vil være TU-løsninger som flere kommuner anvender der identificeres via workshops, er den enkelte kommune selv ansvarlig for at identificere egne TU-løsninger.

Identifikation af egne TU-løsninger

Da organisering, roller og funktioner i kommunerne ikke er ens, kan der ikke entydigt udpeges hvem i kommunen, der skal arbejde med de specifikke delelementer. Nedenstående skal ses som et forslag til hvilke kvalifikationer og faglighed arbejdsgruppen bør have adgang til. Listen er dog ikke udtømmende og andre profiler kan være relevante at inddrage.

Funktion og kvalifikationer, der er relevante for opgaveløsningen i forbindelse med identifikation af egne TU løsninger samt risikovurdering.

- Medarbejder; udpege TU-løsninger igennem kontraktstyringsarkiv
- DPO; kan måske være behjælpelig med at udpege TU-løsninger
- Systemejer for de TU-løsninger der identificeres.
- IT-arkitekt; vurdering af om integrationer påvirkes af TU-løsninger ved omlægning
- Informationssikkerhedskonsulent: hjælpe med risikovurdering

I første trin skal kommunen identificere egne TU-løsninger.

Hvis kommunen ikke har et overblik over egne TU-løsninger, kan alle TU-løsninger findes på følgende måde:

Der findes to tilgange til at identificere alle TU-løsninger:

- Kommunen fremskaffer en liste over alle leverandører med tilhørende aftaler. Dette kan gøres via den centrale eller decentrale kontraktstyringsenhed
    - Når alle kommunens leverandøraftaler er fundet, skal de aftaler der indeholder en TU-løsning identificeres.
    - Det kan være en omfattende opgave at skulle læse alle aftaler igennem, hvorfor det anbefales at der f.eks. søges på nøgleord som NemID, NemLogin, tjenesteudbyderløsning, medarbejdersignatur, m.fl. på alle aftaler. Hvis der findes et kontraktstyringssystem, kan der i dette system evt. søges på tværs af alle aftaler.
- KITOS hvis det anvendes

Når alle TU-løsninger er fundet, kan de løsninger, der er er identificeret som fælles på workshops, fjernes. Herefter bør kun egne TU-løsninger stå tilbage.

Tjekliste for egne løsninger

Når der er tale om en egen TU-løsning, er det den enkelte kommune, der har det fulde ansvar for omlægningen og at løsningen bliver klar til NemLog-in3 (NL3). I tjeklisten nedenfor kommer et bud på en række af de opgaver kommunen skal forholde sig til. Dette skal gennemgås for hver enkelt egen TU-løsning kommunen har.

Uanset om egen TU-løsning er udviklet og driftet af kommunen eller om det sker ved hjælp af evt. underleverandør er det nogenlunde samme opgave. Hvis der er evt. underleverandør tilknyttet, så findes løsningen fortsat kun hos kommunen og ingen andre og skal derfor anses som en egen TU-løsning.

Nedenfor nævnes opgaver som kommunen selv skal varetage eller overveje evt. i samarbejde med leverandør:

1) Kommunen anbefales at orientere sig i de vejledninger og guides Digitaliseringsstyrelsen udgiver via NemLogin omkring testmiljø, integrationer, mm. Da det er kommunens egen TU-løsning, er der behov for at orientere sig i kravene til omlægning og integrationer fra nuværende NemLog-in til den fremtidige NL3. I det omfang integrationen afviger fra standard tilgangen for NemLog-in2.
2) Ved almindelig setup i TU-løsningen håndteres dette i første omgang af Digitaliseringsstyrelsen med en central komponent der oversætter MitID login til et NemID login, når en borger ønsker at tilgå TU-løsningen.

3) Hvis kommunen ikke har et almindeligt setup og opkobling til NemLog-in, skal det vurderes om TU-løsningen skal omlægges til NemLog-in, for at kunne håndtere MitID logon, via Digitaliseringsstyrelsens centrale komponent.
4) Vær opmærksom på, at hvis TU-løsningen har en dokument signerings feature, så virker denne ikke når en borger logger på med MitID via den centrale løsning hos Digitaliseringsstyrelsen. Her skal der udvikles en helt ny feature for at signering fremadrettet virker med MitID.
5) Når NemID lukkes og MitID er det blivende system, skal det vurderes om der er interne integrationer i forhold til f.eks. at der sendes et PID/RID til et internt IT-system. Der skal i snitfladerne omlægges til UUID og de interne IT-systemer skal kunne anvende den nye snitflade.
6) Hvis kommunen centralt har en snitflade, der kalder Digitaliseringsstyrelsens PID/RID service, skal denne også omlægges.
7) Gennemføre risikovurderinger. Dette punkt uddybes senere i rapporten.
8) Der skal indgås ny tjenesteudbyderaftale med Digitaliseringsstyrelsen om opkobling til NL3 Broker.

Mulige tekniske udfordringer for TU-løsningerne

Det er særligt vigtigt at kommunerne er opmærksomme på de tekniske udfordringer der kan opstå ved overgangen fra NemID til MitID.

I det omfang at kommunerne kun anvender den nuværende fælles offentlige NemLog-in2 broker til NemID og Medarbejder Signatur i eksisterende TU-løsninger, så forventer Digitaliseringsstyrelsen ikke der er behov for tekniske tilpasninger i første omgang. Dette vil blive håndteret centralt af Digitaliseringsstyrelsen.

Nogle kommuner har dog valgt TU-løsninger, som afviger fra standardimplementeringen. Her er der en teknisk opgave med omlægninger som skal være på plads, før borgere med MitID kan anvende kommunens TU-løsninger - uanset type. Hvis den enkelte TU-løsning ikke tilpasses, vil borgere med MitID ikke kunne tilgå kommunens selvbetjeningsløsninger. Det forventes at hovedparten af alle TU-løsninger er koblet direkte op på NemLog-in2 broker og at kommunerne derfor kun har få af disse.

Hvis man har en TU-løsning hvor det er muligt at signere dokumenter i, så vil signeringen ikke virke fremover, medmindre kommunen foretager sig noget. Dette uanset om TU-løsningen er koblet korrekt op mod den centrale løsning hos Digitaliseringsstyrelsen eller ej. Med signering vil der altid være en opgave i forhold til en teknisk tilpasning.

Risikovurdering

Formålet med risikovurderingen er, at kommunen på baggrund af denne kan beslutte hvilket sikringsniveau løsningen skal indplaceres på. Det er derfor en vigtig opgave i omlægningen, da risikovurderingen kommer til at danne grundlaget for beslutningen om sikringsniveauet skal være Betydeligt eller Lav, da det forventes at det højeste niveau på kommunalt plan, vil være sikringsniveau Betydelig.

Det er vigtigt at huske at det som udgangspunkt kun er egne TU-løsninger, der skal gennemføres risikovurderinger af, da TU-løsninger flere kommuner anvender anbefales risikovurderet på de fælles workshops.

Ved risikovurdering af egne TU-løsninger anbefales det at følge vejledningen fra Digitaliseringsstyrelsen som kort beskrives her.

I dette link Vejledning til valg af sikringsniveau for tjenesteudbydere 2.0.1 (digst.dk 8. feb. 2021) til Digitaliseringsstyrelsen, findes en vejledning til, hvordan de forventer kommunerne arbejder med, og forholder sig til sikringsniveauerne. Her findes der også eksempler på hvordan de opfatter data og indhold i forhold til de tre sikringsniveauer.

Direkte link til risikovurderingsskabelon

https://digst.dk/media/22432/skema-for-nsis-vurdering-skabelon-v122.xlsx (15.02.2021)

Da antallet af kommunale TU-løsninger, der anvendes af flere kommuner, vurderes til at være meget stort, har KL drøftet risikovurdering af disse løsninger med Digitaliseringsstyrelsen. Efter aftale med Digitaliseringsstyrelsen er det besluttet, at der kan laves risikovurdering på en gruppe af løsninger (pr. forvaltning, leverandør etc.) ligesom der kan foretages en mere simpel risikovurdering end Digitaliseringsstyrelsens vejledning angiver.

Simpel risikovurdering for TU-løsninger flere kommuner anvender

Kommunernes medarbejdere behandler en lang række følsomme og fortrolige oplysninger om borgerne i deres daglige brug af it-løsninger.
Konsekvenserne for borgerne, hvis disse oplysninger tilgås af forkerte, kan være alvorlige.

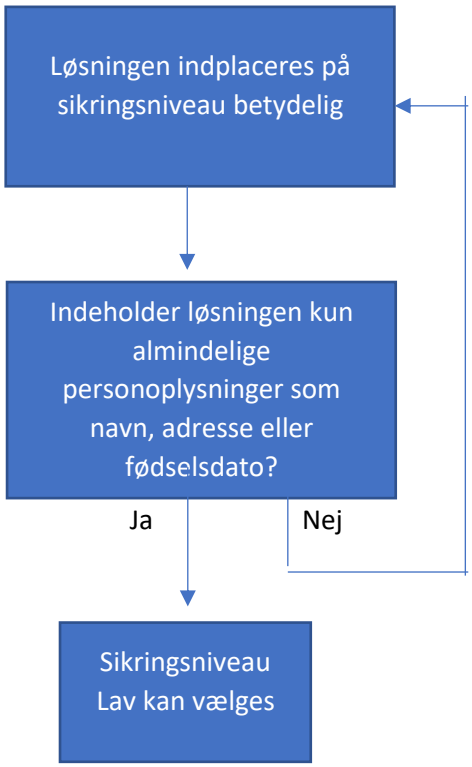
Ligeledes er der en række borgervendte selvbetjeningsløsninger, der kan indeholde følsomme og fortrolige oplysninger om borgeren, hvor det er vigtigt at sikre, at ikke andre end borgeren selv har adgang.

Med det afsæt vil det være forventeligt, at langt de fleste kommunale løsninger vil blive risikovurderet således, at de vil skulle indplaceres på sikringsniveau Betydelig.

For at minimere arbejdet med at skulle risikovurdere samtlige kommunale TU-løsninger detaljeret, kan de indplaceres direkte på sikringsniveau Betydelig.

Hvis løsningen kun behandler almindelige personoplysninger som navn, fødselsdag og adresseoplysninger på borgerne, kan den indplaceres på sikringsniveau Lav efter en nærmere vurdering.

En løsning, der kan indplaceres på sikringsniveau Lav, kan eksempelvis være ”En kommunal tjeneste til bestilling af ekstra skraldespande” eller ”Indberetning af forbrugstal til el, vand varme mv.”



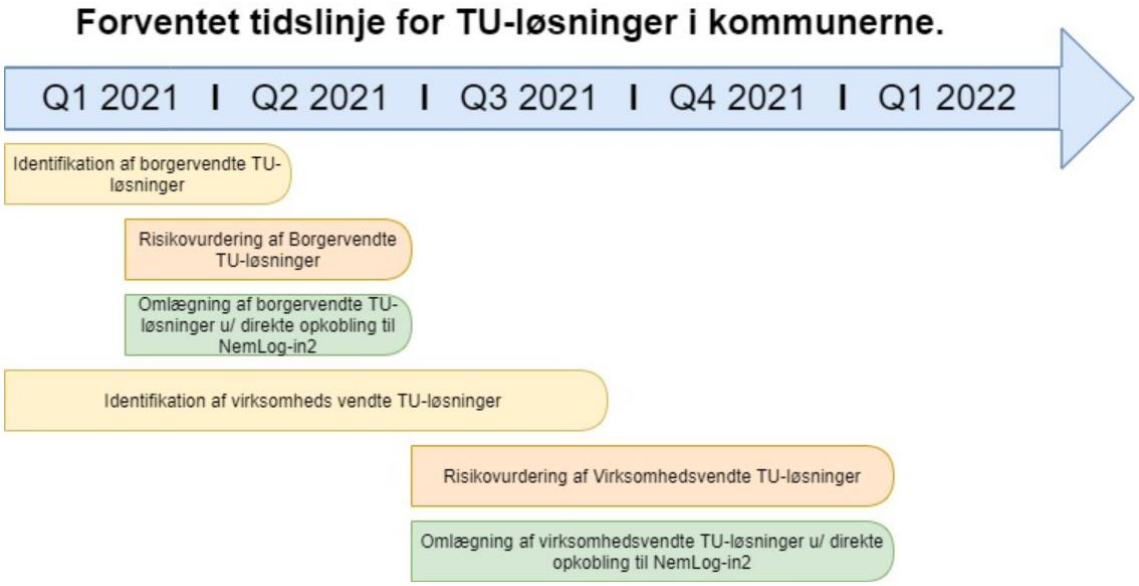
Eksempel på en mere detaljeret risikovurdering

Som eksempel på en risikovurdering fra KOMBIT er der vedlagt en risikovurdering af SAPA.
Vær opmærksom på at der i eksemplet er udarbejdet to risikovurderinger, da der er tale om to usecases.
Kommunerne kan her se hvordan fremtidige risikovurderinger kan se ud, eller give inspiration til hvordan risikovurderinger af egne TU-løsninger kan udarbejdes.

I Bilag 5 kan der læses yderligere om eksemplet.

Tidsfrister for omlægning af TU-løsninger i kommunerne

Tidsfristerne for omlægning af kommunernes TU-løsninger skal inddeles i TU-løsninger der er målrettet henholdsvis borgere samt TU-løsninger til virksomheder og ansatte i kommunerne.



Digitaliseringsstyrelsen skriver følgende på deres hjemmeside:
"Et overordnet hovedprincip for migreringen er, at migrering af tjenesteudbydere påbegyndes inden migrering af slutbrugere. Leverandøren for NemLog3-in skal levere en migreringsplan for tjenesteudbydere og brugerorganisationer." Digitaliseringsstyrelsen[1])

Endvidere har Digitaliseringsstyrelsen meddelt, at de fra centralt hold udvikler en løsning som konvertere et mitID logon til et NemID logon. Det vil sige, at for alle kommunerne hvor man har en TU-løsning der er koblet direkte op til NemLog-in2 Brokeren, håndteres overgangsperioden automatisk.

For de borgerrettede TU-løsninger, der ikke håndteres centralt af Digitaliseringsstyrelsen, er det forventningen at kommunerne skal have omlagt disse primo august 2021. Det er vigtigt at være opmærksom på, at har kommunerne TU-løsninger, hvor der skal signeres dokumenter, så vil signeringen ikke virke, hvis en borger logger på med MitID. Dette da OCES-certifikatet, som bruges til signeringen, udgår. Her skal derfor bygges en ny løsning som håndtere dette.

Det betyder endvidere at alle TU-løsningerne i kommunerne målrettet virksomheder i kommunen, skal være omlagt primo januar 2022 hvor overgangsperioden for erhvervsrettede TU-løsninger forventes at opstarte.

Det anbefales derfor at kommunerne først fokuserer på de TU-løsninger, der er målrettet borgerne.

Delrapport 2

Kommunernes opgaver forbundet med at implementere NSIS falder i fire grupper:

1. TU-løsninger (indgår i delrapport 1)
2. Etablering af IdP
3. Ekstern brugerstyring i forhold til fællesoffentlige løsninger og
4. Borgerservice

I næste rapport til kommunerne omkring NSIS-projektet, sættes der fokus på opgaverne 2-4, som alle medfører en række opgaver og investeringer.

I dele af kommunikationen fra Digitaliseringsstyrelsen, er der i højere grad fokus på selve løsningerne end på den indvirkning NSIS får for kommunernes organisation og kommunernes IT-anvendelse mere bredt. Delrapport 2 går bredere ind i de opgaver, kommunerne skal fokuser på.

Der ses fire overordnede områder kommunerne skal arbejde med i relation til NSIS:

1. TU-løsninger

Som det fremgår af denne rapport, er der et arbejde i og omkring kommunernes TU-løsninger. Det anbefales at denne rapport benyttes som tilgang til arbejdet i kommunen.

2. Lokal IdP i kommunerne – intern brugerstyring

NSIS stiller krav til måden kommunerne driver en Lokal IdP. Kravene retter sig både mod den tekniske løsning og mod kommunens organisation. De tekniske opgaver minder om opgaver kommunerne har arbejdet med før. Den organisatoriske del af det vurderes som en ny opgave. Det er vigtigt, at kommunerne vælger en teknisk løsning, der understøtter den organisatoriske opgave. Den tekniske løsning der vælges, vil i høj grad have indflydelse på omfanget af de opgaver, der skal løses i organisationen.

Deadline for at implementere en lokal IdP-løsning er ultimo 2021. Det forventes, at der vil være en parallel drift i første halvår 2022.

Mange kommuner fokuserer allerede på etablering af lokal IdP og der er hos flere kommuner udarbejdet isolerede NSIS-Gap analyse for dette specifikke arbejdsområde vedr. IdP løsninger.

I Delrapport 2 kommer rapporten nærmere ind på de muligheder og udfordringer, der kan være ved at vælge at anskaffe den rigtige løsning og de mulige faldgruber der kan være ved at ville udvikle en egen IdP løsning.

Delrapport 2 kommer endvidere ind på de udfordringer der er, og de beslutninger der skal tages i forhold til, om man som kommune skal anvende en eller flere IdP løsninger i kommunen.

3. Fællesoffentlige løsninger – ekstern brugerstyring

Dette arbejde skal opstartes ultimo 2021, umiddelbart efter der er etableret IdP løsning/løsninger hos kommunen.

Konkret er der tale om at kommunerne anvender en række fællesoffentlige portaler som Fælles medicinkort, virk.dk m.fl. hvor der skal ske oprettelse af medarbejder når de overgår til den nye MitID erhvervssignatur og deres nuværende medarbejdersignatur lukkes.

4. Borgerservice

Borgerservice skal være klar til at supportere og arbejde med udstedelse af MitID og support af MitID i pilot overfor borgerne pr. 14. juni 2021 i henhold til den nuværende plan fra Digitaliseringsstyrelsen.

Her får kommunerne retningslinjer, procedurer mv. fra Nets i forbindelse med at kommunerne indgår i en ny RA-aftale for MitID.

Bilag

Bilag 1: Overblik over besvarelser fra analysen

Hvis kommunen er i tvivl om hvordan den ligger, sammenlignet med andre, gives der her et kort overblik over de mest gængse svar. Så kan kommunen selv vurdere hvor ens den ligger med de andre.

Det er svært at placere en kommune som værende gennemsnitlig, da det afhænger af hvilke data der tages udgangspunkt i. Flere kommuner har besvaret at de har 100+ TU-løsninger, men ved gennemgang af løsningerne, viser det sig at det er blanketter bag selve TU-løsningen. Andre kommuner har angivet at de kun har en eller to TU-løsninger. Derfor er det svært at komme med et bud på om der findes et gennemsnit på antallet af TU-løsninger.

I spørgsmålet om hvorvidt kommunerne forventer at skulle bruge sikringsniveau Høj, svarer langt over halvdelen at de ikke forventer det. Dette stemmer overens med anbefalingerne for sikringsniveauer, da det vil være et fåtal, hvis der overhovedet er brug for niveau Høj i første omgang.

11 kommuner har angivet at de er gået i gang med arbejdet med at få kortlagt og planlagt om det er kommunen eller leverandøren, der står med omkostningen for omlægningen af TU-løsningen. Det viser også et billede af at mange kommuner endnu ikke vurderes at være startet på denne opgave endnu.

Størstedelen af alle kommuner har endnu ikke besluttet hvilken skabelon der skal bruges til at lave risikovurderinger. De kommuner der har taget stilling til det, forventer alle at bruge Digst (Kombit), mens en enkelt forventer at bruge egen NSIS-risikovurderings ramme.

I forhold til at tage stilling til hvordan systemer skal tilpasses i forhold til afskaffelsen af PID/RID, ses det at størstedelen af alle kommuner endnu ikke er startet på arbejdet. Et fåtal angiver at de har startet arbejdet, men ingen har afsluttet opgaven.

Bilag 2: Metode og dataindsamling

Metode

Al data er indsamlet kvantitativt, for at sikre sammenlignelige svar til brug for den efterfølgende analyse. Tilgangen for undersøgelsen, har været at gøre det så simpelt som muligt, og kun indhente de informationer der er nødvendige for projektet. Spørgeskemaet er udarbejdet, så det både dækker status på den enkelte kommunes fremgang med NSIS, men også for at give en status på de kommuner, der endnu ikke er startet på projektet. Dette for at give et samlet overblik for alle 98 kommuners fremgang.

Spørgeskemaet er inddelt i to overordnede emner, hvor der først søges at skabe et overblik over samtlige tjenesteudbyder løsninger i Danmark. Dette med henblik på at kunne udpege top-5 af disse. Dernæst følger en række spørgsmål der sikrer hvilke forventninger kommunerne, har til fremtiden indenfor IdP, så der bliver skabt et datagrundlag for GAP-analysen, uden at skulle bede kommunerne udfylde to forskellige undersøgelser.

Undervejs i processen med udarbejdelsen af spørgeskemaet, er spørgsmålene sendt til både styre- og arbejdsgruppen for NSIS-projektet, så de fik mulighed for at komme med input og feedback. Dette har sikret forståelige spørgsmål, samt klarhed over hvad der kunne forbedres inden spørgeskemaet blev sendt ud. Udsendelsen blev sat til den 16.12.2020 og deadline for besvarelse var sat til 15.01.2021. Denne blev dog rykket til primo februar, grundet manglende svardeltagelse.

Datagrundlag

Spørgeskemaet er sendt til alle 98 kommuner i Danmark, hvoraf 55 er vendt tilbage med besvarelser. Svarprocenten der ligger på 56 %, vurderes, at den er tilfredsstillende, da den sidste del af besvarelser ikke antages at komme med en stor ændring i antallet af TU-løsninger, eller frembringe andre end de allerede nævnte TU-løsninger.

Bilag 3: Total liste over alle TU-løsninger som flere kommuner anvender

I listen oplyses alle TU-løsninger som flere kommuner anvender på tværs af alle eller flere kommuner. Listen indeholder ikke TU-løsninger som kommuner har oplyst som egne.

Alle TU-løsninger oplyst af kommunerne, uden de er nærmere kontrolleret eller valideret. Listen skal derfor tages med forbehold for at der kan være afvigelser i forhold til rapportens tilgang til TU-typer.

ACmatch	CPRWeb
Adresseforespørgsel	CSC
AffaldOnline.dk	Cura - Systematic
Afvis journaloverdragelse - DXC	Dafolo
Akutrefusioner	Daycare
Al dente	DDB - Danskernes Digitale Bibliotek
AlmenByg	Deltager fra anden kommune (voksenundervisning)
Anden Aktor Portal (AAP)	Det Fælleskommunale Selvbetjeningstjek
Anmeld flytning til folkeregisteret - DXC	DIADEM
Anmeld flytning til udlandet (udrejse) - DXC	Diaform - Dafolo
Anmeld flytning til udlandet (udrejse) fra DXC	Digirehab
Ansøg om navne- og adressebeskyttelse - DXC	Digital flytning
Ansøg om navne- og adressebeskyttelse fra DXC	Digital Forløbsguide
Anvendelse af offentlig arealer. bookingsystem	Digital Pladsanvisning
Apinux Healthcare	Digital Post
Arkibas	Digitalt Fremmødesystem (DFR)
as	Digora
Aula	DitmerFlex
Barnets bog	DKPlan (DIgital Kommuneplan)
BBR	DoseSystem
Bestil bopælsattest	DUBU - Kombit
Bestil nyt sundhedskort - DXC	DXC Technologi Scandihealth
Bibliotecha	E-Arkiv
Bibliotek.kk.dk	e-arkiv (sagsakter fra amterne) Miljøportalen
Biometric Solutions	EASY
Bluewhale	Easy.dk
BO Skærm Kube Capture	EasyIQ Office 365
Boliglånesystemet	Easypark p-licens
BOM	E-boks
Borger.dk	Edora Workforce Planner
Borgerbilledet	Eduadm - Ditmer
Borgerblikket	Edulife
Borgerbooking	E-flyt - DXC
Borgeronline.dk	E-flyt - Scandihealth
BOSSINF-STB WEB	EG
BVL Solteq	EG Lån til beboerindskud
Byg og Miljø - Kombit	EG Netblanket

Bygningsaffald.dk/SWECO. byggeaffald – anmeld	EG Netforvaltning
Bygselv (50+ mindreløsninger)	EG Netforvaltning Sundhed
BørneIntra	EG Netforvaltning Vielse
Børneungeliv.dk	EG OIB Borger
Bådregistrering i Gudenåens bådregister	EG On Helbredstillæg
Cicero - Systematic	EG Selvbetjening
Comdia	EG Sensum
Conventus booking	EG Smartdesigner
CPR/Folkeregister	EG Speciallæge- og Psykologdatabasen MediConnect
CPR-selvbetjening	egen adfs
Ejendomsregistreringsportalen	JordWeb
Emento Digital Forløbsguide	JOSA
Emento Sikker Dialog	Kasseregistrerings/Betalingssystem
Emply (rekrutteringssystem)	KbhBarn
Emply Project	Klageportalen på Nævnenes Hus
Energykey	KLE - Byg og Miljø
EnergyProjects	KLs blanketlicensordning
E-protokol	KMD
Erklæring fra fodplejer/fodterapeut	KMD Boliglån
Exorlive	KMD BossINF
Famly Kommunikationsplatform	KMD Civis Basis
FFT (Functional Family Therapy)	KMD Digital Pladsanvisning
FilArkiv	KMD ESR
FirstAgenda	KMD Institution
Fjern person fra min adresse - DXC	KMD løsninger
FLIS (Fælleskommunalt LedelsesInformationsSystem)	KMD MinUddannelse
FMK - Fælles Medicinkort	KMD Nexus
Fokus	KMD Nova Link
Fordelingskomponenten (STS)	KMD Opus
Frame	KMD Pladsanvisning
Front Desk ApS	KMD Social Pension
Frontdesk tidsbestilling	KMD Strucktura
FUT Platform	KMD UVVej
Fælles Biblioteksystem FBS	KMD Valg
Fælles Medicinkort (FMK)	Kommunebetaling
Fælleskommunal løsning på Miljøportalen	Kommunernes Sygedagpenge KSD
Generelt - selvbetjening.id-port.dk	Kommunernes Ydelsessystem KY
Genoptræn.dk	Kontakt Lægen
Geo Environ	KUBE
Grundlisten	Kultunaut
Hal Booking	Kørekort og pas
Hjernen & Hjertet Forældreportal - Rambøll	Køreprøvebooking
HjerteKomMidt	Køreprøvebooking - Kombit
HR-skyen Rekrutteringssystem	Landbrugsindberetning.dk
Husdyrgodkendelse - Miljøstyrelsen	LARA
Hypernet for dagtilbud	LER (Ledningsejerregistret)

iBinder	Letdialog
IHM Care	Leverandørplatformen
Indsigsret	Liva
InsuBiz	Lokalebookning. Aalborg bibliotekerne
intra.mariagerfjord.dk	Lokalplanportalen
Intranet - rettet mod kommunes ansatte	Ludus Suite
ISAP-skadeanmeldelsesystem	Lægeskift - Scandihealth
IT-sikkerhedserklæring	Lægevalg - DXC
JobAG	Lån til betaling af ejendomsskat
Jobcenter Planner	Maneno
Jobnet.dk	MasterCater
mDoc FM	RMG C3 Forsikring
Medarbejderadgang	Rottegis Tip kommunen
Meebook	Rotteweb - Sweco
Min Institution	Saftynet
Min Kommune (Fujitsu debitor)	Sags- og Partsoverblik - SAPA
Min Sag	Samtykke til indhentning af referencer
Min Sag. Dataproces	SBSIP
Min Side - Digital flytning	SBSYS
MinSag - Dataprocess	Schultz Booking
Mit betalingsoverblik	Schultz Connect
Mit sygefravær	Schultz FASIT
MoEva	Schultz Forum - mobil app
Nem refusion	Schultz Jobspor
NemId.nu	SD løn
NemKonto	Se din ejendomskattebillet - KMD
NemKonto Tilslutning	SEI (Sundhedsdatastyrelsens Elektroniske Indberetningssystem)
Nemrefusion - Kombit	Sekoia
NemTilmeld	Selvbetjening.nu
Netblanket	Selvbetjeningsautomater
Netforvaltning - offentlige arrangementer	Seneste lægeskift / journaloverdragelse - DXC
Netic	Serviceplatformen
Nordjyllands Beredskab intranet	Signatur On- & Offboardingsystem
NOTUS	Signatur Rekrutteringssystem
Notus - DXC	Signaturgruppen
Novax	Skat.dk
Ny parkeringsbutik	Skift kode
Optagelse.dk	Skift læge
OS2autoproces	Skift sikringsgruppe - DXC
OS2faktor	Skiftadgangskode.mariagerfjord.dk
OS2Forms	Skolebod.Vejle.dk
OS2Indberetning	Skoleintra.IST Learning
OS2nykode	SKS fremmøde
P afgift klagesystem	SKS løntilskud
Pasning og Skole	SKS/SKA Application
Password reset	Socialt frikort - Kombit

Password reset med NemID	Sofus
P-automat afmelding	Sofus match
Pilotafprøvning af PRO	Solo ID. Signaturgruppen
Plan2Learn	Solrød Kommune Betalingskort
Plandata	SpeedAdmin
POC	STAR løsninger
Prisme (Borgerportal)	Sundhed.dk
Prisme Fujitsu	Sundhedstjenesten
Prisme udbetaling	Sundhedsvejen.dk
Pårørende-app	Sweco Park
RenoWeb	Sygesikring
Renowork	Søg adresseoplysninger på person -DXC
Tabulex	
Tand BVL - Solteq	
Tandplejen Vesthimmerland	
Tandplejens book-selv	
Telesår/Pleje.net	
Tidsbestilling	
Tilmelding til sommerferieaktiviteter	
Tinglysning	
TK2	
TK2 - Borgerbooking	
TK2 - Tandplejesystem	
TM Tand	
TMF Erhvervsportal	
Udstedelse af NemID (medarbejder login)	
Uno STU	
Uno Ung	
Valghalla 2.0	
Valgsystem/valgweb	
Vejman.dk	
Virk.dk	
Vis min sygesikringsoplysninger - DXC	
Vis mine sygesikringsopslysninger - Scandihealth	
Vitas	

Bilag 4: Liste fra KITOS samarbejdet med IT-systemer

I listen nedenfor findes alle de systemer der er registreret på tværs af KITOS samarbejdet. I listen gengives alle de systemer som har 20 eller flere kommuner som anvendere.

Bemærk da Vangsaa Consult ikke kender alle systemerne, kan der være en række systemer i listen som ikke er TU-løsninger. Men listen ses stadig som en god mulighed og som en kilde til hvilke systemer kommunerne skal undersøge nærmere i forhold til om der er tale om et TU-system.

Herudover indeholder listen en lang række fælles offentlige systemer, som også kan være relevante at udpege. Disse har dog ikke noget med kommunens TU-arbejde at gøre, men skal bruges på et senere tidspunkt. Der kommer nærmere forklaring på dette i delrapport 2.

OS2KITOS	KMD Børneydelse
KMD AKTIV	KMD Structura
KMD Doc2Archive	KMD OPUS Energi / Easy Energy
KMD Doc2mail (OneTooX)	QGIS
KMD Sag	KMD Gennemstilling via KMD-net
Byg og Miljø	Uno Ung
Digital Post	KMD NemKonto
KMD Indkomst	VandløbsGIS
KMD LOS	Mapinfo
EG Netforvaltning Sundhed	NOTUS Adresseforespørgsel og bopælsattest
KMD KSP CICS	EG Selvbetjening Smart Designer
FirstAgenda	Place2Book
Fælles Bibliotekssystem (FBS)	TM Tand
FLIS (Fælles LedelsesInformationsSystem)	KMD Social Pension - Kommune (KMD SPK)
BBR (Bygnings- og Boligregistret)	SignFlow Sikker Mail (SIKKER@MAIL)
Digitaliseringskataloget	WorkForce Planner - WFP
EG Speciallæge- og Psykologdatabasen MediConnect	DriftWeb
SAPA - Sags- og Partsoverblik	DPR Register
Danmarks Miljøportal	Microsoft Office Visio Standard
KMD Udbetaling	Diaform+
KMD Social pension	MeeBook
DAR - Danmarks AdresseRegister	FK Ydelsesindeks
SpeedAdmin	CD-ORD
Novax Sundhed	Autodesk Revit
KOMBIT Køreprøvebooking	Micosoft Windows Internet Explorer
KMD P-data	SkoleKom
KMD Structura Ejendomsskattelån	NOTUS Kommunal
Kommunernes Sygedagpengesystem (KSD)	Borgeronline®
KMD Boliglån	FilArkiv
NemRefusion	KMD OPUS Business Intelligence
KMD ESR (Ejendomsstamregistret)	ArcGIS

KMD Arkivering	KMD Structura Byggesag
Kommunernes Ydelsessystem (KY)	KMD BOSSINF
AULA	KMD Indkøbsanalyse
KMD V-data	FK Sags- og Dokumentindeks
Borger.dk	DKplan (Digital Kommuneplan)
KMD Institution	Novax Sundhedsvejen
Signaturcentral	WISC
Digital flytning	Adobe Indesign
KMD OPUS Økonomi	Adobe Creative Cloud
Civis Pas og Kørekort	KMD Navn og Adresse
EG NetForvaltning Vielse	Feliks
DUBU (digitalisering udsatte børn og unge)	FVDB Fælleskommunal Virksomhedskontakt Database
KMD Valg, Valgudskrivning	KMD KFS-LAN/NT
KMD Valg, Valgopgørelse	Citrix Receiver
KMD OPUS Debitor	Master Cater System
Rotteweb	UNI•Login Brugeradministration
KMD NemAdgang	InsuBiz
KMD Nexus	TEA Forvaltning
Ydelsesrefusion	KMD Kommunikationskapacitet til KMD-net
Vejman	KMD Distributionscenter
Hjernen og Hjertet	KMD Valg, Stemmeoptælling
Mit Sygefravær	Acadre MM
CPRWeb	Medcom
DDB - Danskernes Digitale Bibliotek	KMD Børn og Voksne
Selvbetjening.nu	TOPdesk
Schultz KommuneKoncept	KL emnesystematik (KLE)
Microsoft Office 365	EjdExplorer
SurveyXact	Cisco Anyconnect Client (VPN)
KMD OPUS Koncernstyring	KMD Tandpleje
VITAS - Digital ansøgning	KMD Care
Tabulex Elevadministration (TEA)	OS2 Rollekatalog
KMD Civis Basis	Google Chrome
KMD Valg	Computopic Gruppe-SMS.dk
KMD Host Print Facility	DIBS (Internet basis betalingsløsning)
KMD Dagpenge	Adoxa
EG Netblanket	Alinea Fagportal
Tabulex Trio Tjenestetid	KMD OPUS Personale, Fravær
KMD Admin	Dansk Skoleskak
Microsoft Active Directory (AD)	Arkibas 5
Virk	Microsoft Office Publisher
GeoEnviron	KMD AKTIV Timeregel
SkoleIntra	Microsoft Windows 7
KMD EDI service	Uno Brobygning
Strålfors Connect	Citrix XenApp
EG OIB Borger	Open+

KMD OPUS Personale	CSC Sygesikring
FrontDesk	KMD Budgetweb
KMD OPUS Brugerstyring	Plan2Learn, Kursusadministrationssystem
eReolen	KMD ZSRØR
Dynamic Template	SBSIP
KMD OPUS Rollebaseret indgang	KMD OPUS Vagtplan
Borgerblikket	DaluxFM
TeamViewer	Microsoft Office Project Standard
KMD P-data online	TARGIT Decision Suite
Telesår/Pleje.net	KMD AKTIV Ledighedsydelse
Socialt frikort	KMD EKJ (Elektronisk Klientjournal)
VinterMan	Password Reset med NemID
NOTUS eBorger	Adobe Photoshop
LARA	CSC Tinglysning
SkoleTube	Siteimprove Quality Assurance
KMD Cognito Local	Tabulex SFO Børn
VASP	KMD Educa Elev
KMD OPUS Data	Colourbox.com
KMD Fokus	OS2Valghalla
KMD Sag Journal	SD Løn
Secure ISMS	KMD Cognito Access
UdlændingeInformationsPortal, UIP	VejVejr Glatførevarslingssystemet
FK Administrationsmodul	Mermaid
Nets RA-portalen	LOIS Statistik
Schultz FASIT	Valg
EG NemJournalisering	KMD Structura Ejendomsskattelån, eAnsøgning
DPSD - Dansk Patient SikkerhedsDatabase	Concierge Booking Software
RenoWeb	Umbraco CMS
Skype for Business	KMD BørneIntra
JordWeb	NemTilmeld
KMD Filforsendelse System (KFS)	Digora
KMD Institution - Digital Pladsanvisning	KMD OPUS Personale, Tjenestemandspension
TK2	Tunstall Tryghedscentral
Arbejdsmarkedsportalen	Novax Danmarksbørn
Clio online	KMD Aktiv Korrektion
Plandata.dk	KMD Structura Ejendom
VAR Healthcare	Karnov On-line
Tabulex Skema	IntraNote Portal Server
LOIS	Sundhedsdatanettet, SDN
Fælles Medicinkort (FMK)	Fælles Biblioteksinfrastruktur (FBI)
KMD Vagtplan	Dream Broker Studio
Ordbogen.com	Rambøll Sprog
ExorLive	KMD Sag EDH
TN3270	Spatial Suite - Entreprise WebGIS
Emply Hire /Emply Recruitment	Prisme
KMD Institution - Prokap	SMS Passcode

Microsoft Office Outlook	Princh
FK Fælleskommunal infrastruktur	BookBites
Demografix	EG Netforvaltning Sundhed, Korrespondancemodul
Scandi System Pas og Kørekort løsning	ESR Ejendomsskat
NOTUS eBorger - eFLYT	Mercell
kMastra	OS2autoproces
FK Organisation	VMware VirtualCenter Server
EG Sensum Bosted	SEPO Sikker Mail
KMD Valg, Valgudskrivning, digital valgliste	Skoledu.dk
Skat eIndkomst	Digital Post Administrationsportal
KMD Momentum	DPR Viderestilling
KMD Kommunal Medfinansiering (KMF)	RoSy DIGWEB
Computopic SMS Gateway	Ejendomsskat- og Ejendomsbidragssystem
WebLager	Microsoft Windows 10
Skyfish	Salto Adgangskontrol
Tabulex Webindskrivning	Siteimprove Accessibility
AutoCAD	Tabulex Fravær
Matematik Fessor	EG OIB Borger, Ansøgning om udvidet helbredstillæg
KMD Sag Administration	KortInfo Niras
FK Adgangsstyring for brugere	RoSy®
Rakat	Tabulex Ekstrakt
SBSYS	CICERO Move
Biometric-optag	DMS Hjælpemidler
Jobcenter Planner	EG Sensum InCorp
Digital Signatur	Tidsadministration
EG Selvbetjening	KMD OPUS Single Sign-on
KMD Institution - Dagplejemodulet	EduAdm
Microsoft Office Excel	DBD - Vedligehold
UVVej	Columna Cura
Gyldendal Fagportalen	FK Fordelingskomponent
KMD Valg, Valgudskrivning, brevstemmeprotokol	KMD Opera Univers
Microsoft Office Word	Kultunaut
Microsoft SQL Server	CVR
NOTUS Adressebeskyttelse	KMD Institution - Økonomisk Friplads
Klassetrivsel.dk	GeoEnviron Tidsregistrering
KOMBIT Social Pension	KMD Klientbetaling
FK Beskedfordeler	ADFS S-token basis
FK Klassifikation	Newsdesk
SKATs myndighedsnet (ekstranet)	Kingo
Siteimprove Analytics	KMD Educa Personale
ADFS (Active Directory Federation Services)	MailChimp
Det fælles datagrundlag (DFDG)	KMD Vejviser
MinUddannelse	KMD OPUS Personale, Personaledokumenter
FK Adgangsstyring for systemer	Tilbudsportalen
Acadre	Diaform+ Vielse
KMD OPUS Løn og Personale	KMD OPUS Debitor Journal og advis

Børnungeliv.dk	Schultz LovGuide Guide
Jobnet.dk	FrontRead
eDagpenge Sygdom	NOTUS e-Sygesikring

Bilag 4: Eksempel på KOMBIT risikovurdering af SAPA

I vedhæftningen til denne rapport findes 3 dokumenter som til sammen udgør et eksempel på en risikovurdering i Digitaliseringsstyrelsens skabelon for risikovurdering af en TU-løsning.

Husk årsagen til der er to risikovurderinger er, at der i SAPA er to usecases.

Excel: 1. Skema for NSIS-vurdering – SAPA – Administrator v.1.2

Excel: 2. Skema for NSIS-vurdering – SAPA – Sagsbehandler v.1.2.

Disse to excel dokumenter viser selve risikoskemaet, samt hvordan de bliver udfyldt.

Word dokument: 3. Dokumentation af NSIS-risikovurdering og sikringsniveau – SAPA v.1.1. Dette viser den skriftlig dokumentation, som alle kommuner skal udarbejde for de enkelte TU-løsninger.