DAGSORDEN

TEMA: SAMTÆNKNING OG OPTIMERING AF BRUGERSTYRING

IT-ARKITEKTURRÅDET

Dato: 24-04-2024 09:30
Sted: KOMBIT, Halfdansgade 8, lokale Vadehavet

'Rammearkitekturen er fundamentet for, at kommunerne anskaffer effektive digitale løsninger, der styrker den kommunale opgaveløsning og skaber sammenhæng på tværs. Det sker med borgeren i centrum og på et åbent marked.'

Vision for den fælleskommunale rammearkitektur, vedtaget af Kommunernes It-Arkitekturråd februar 2017.

1. Dialog med KL’s direktion

1.1. Dialog med KL's direktion

SAG-2023-03577

Baggrund

’Dialog med KL’s direktion’ er et fast punkt på It-Arkitekturrådets møder og har direktør Christian Harsløf som deltager.

Punktet har til formål at understøtte, at arkitekturdrøftelser og -anbefalinger og den generelle digitaliseringsdagsorden kommer tættere på KL’s direktion.

Indstilling

Sekretariatet indstiller, at It-Arkitekturrådet

- tager direktionens orientering til efterretning.

Sagsfremstilling

2. Siden sidst

2.1. Siden sidst

SAG-2023-03577

Baggrund

Indstilling

Sagsfremstilling

3. Drøftelsessager

3.1. Orientering om arbejdet med Fællesoffentlig Digital Arkitektur

SAG-2023-03577 Her skrives ansvarliges initialer

Baggrund
Den fællesoffentlige digitale arkitektur udarbejdes og vedligeholdes i et fællesoffentligt samarbejde i regi af 'Digitalisering der løfter - fællesoffentlige digitaliseringsstrategi 2022 – 2025' og Regeringens digitaliseringsstrategi 2024-2027.

Indstilling
Sekretariatet indstiller, at It-Arkitekturrådet:

- tager orienteringen til efterretning
- giver input til det videre arbejde

Sagsfremstilling
Digitaliseringsstyrelsen ved Kontor for teknologi og data giver på mødet en orientering om aktuelle indsatser og projekter, der gennemføres i regi af Udvalget for Arkitektur og Standarder.

3.2. Introduktion til arkitekturvinkler på brugerstyring

SAG-2023-03577 Peter Falkenberg og Vibeke Normann

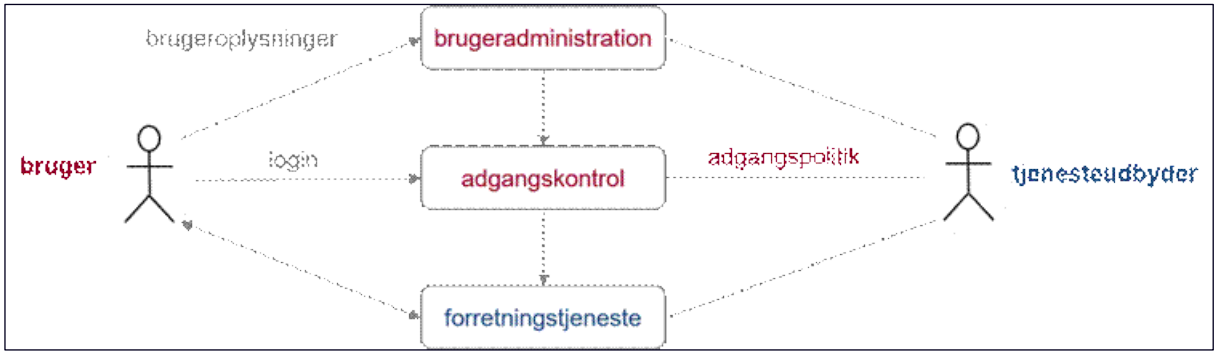
Baggrund
At have styr på hvem der er hvem, og hvad de må se og gøre, er fundamentalt i en organisation. Denne disciplin har altid været nødvendig, men digitalisering af processer og information samt en række yderligere omstændigheder har nødvendiggjort en større og mere fokuseret indsats.

Nogle af de aktuelle forhold der spiller ind i forhold til myndighedernes bruger-styring, er bl.a. en tiltagende grad af arbejdsdeling og samarbejde på tværs af myndigheder, der stiller nye krav til en sammenhængende styring af brugerne. Med cybertrusler og en øget mængde af dataangreb, presses der yderligere på for, at datasikkerheden er i orden hos myndighederne,

hvilket også er helt centralt for at sikre tilliden til det offentliges håndtering af borgernes data. Med nye og flere lovgivningskrav omkring beskyttelse- og adgang til data, som fx GDPR, følger der også nye og strengere krav til håndteringen af brugerne.

Dagens tema omkring brugerstyring har derfor til formål at komme omkring nogle af de aktuelle indsatser, de tilhørende udfordringer og få drøftet mulige fremtidige tiltag.

HVAD er brugerstyring
Definition:
Brugerstyring omfatter administration af identiteter og adgangskontrol:



HVORFOR brugerstyring
Brugerstyring er en integreret del af en organisations sikkerhedsstrategi og hjælper med at skabe et sikkert og pålideligt it-miljø.
Styring af medarbejderes adgang til it-systemer er afgørende af flere årsager:

- Datasikkerhed: Adgangsstyring hjælper med at beskytte fortrolige oplysninger og data mod uautoriseret adgang. Ved at begrænse adgangen til kun de nødvendige personer reduceres risikoen for datalækager, misbrug eller tyveri af følsomme oplysninger.

- Overholdelse af lovgivning: Mange offentlige organisationer er underlagt specifikke lovgivninger og reguleringer, der kræver beskyttelse af personlige oplysninger og data. Effektiv adgangsstyring er afgørende for at overholde disse lovgivninger og undgå bøder eller juridiske konsekvenser.

- Forebyggelse af interne trusler: Adgangsstyring hjælper med at minimere risikoen for interne trusler, hvor medarbejdere bevidst eller ubevidst kan forårsage skade på systemet eller misbruge data. Ved

at begrænse adgangen til de nødvendige ressourcer kan man minimere potentialet for skadelig adfærd.

- Beskyttelse mod eksterne trusler: Adgangsstyring hjælper også med at forhindre uautoriseret ekstern adgang til systemer. Dette er især vigtigt i en tid, hvor cybertrusler og angreb er stigende. Effektiv adgangsstyring kan fungere som en barriere mod uautoriseret adgang fra udenforstående.

- Revision og sporbarhed: Adgangsstyringssystemer giver mulighed for at overvåge og registrere aktiviteter, hvilket gør det lettere at følge medarbejdernes handlinger og identificere eventuelle uregelmæssigheder. Dette er værdifuldt for revision og efterforskning i tilfælde af sikkerhedsbrud eller fejl.

Indstilling
Sekretariatet indstiller, at It-Arkitekturrådet:

- Tager introduktionen til efterretning

Sagsfremstilling
Når vi skal forholde os til brugerstyring på det kommunale område, kan vi på strategisk niveau støtte os til de 5 fælleskommunale arkitekturmål, jf bilag, og den fællesoffentlige referencearkitektur for brugerstyring, jf bilag. Referencearkitekturen indeholder bl.a. 6 principper for brugerstyring og beskriver 5 arkitekturmønstre for brugerstyring, fra den mest enkle type (en forretningstjeneste med egen autentifikationstjeneste) til den mere komplekse (føderation mellem flere domæner).

Principperne for brugerstyring er:
1. Brugerne oplever en relevant og sammenhængende adgangsstyring.
2. Brugerstyringsløsninger respekterer brugernes privatliv.
3. Tjenesteudbyder har ansvaret for at adgangspolitikken håndhæves.
4. Brugerstyring er adskilt fra forretningstjenester.
5. Brugerstyring realiseres via løst koblede og standardiserede tillidstjenester.
6. Tjenesteudbydere indgår i føderationer.

Principperne fokuserer på følgende gevinster:

1. En sammenhængende adgangsstyring skal gøre **medarbejdere og borgere** mere tilfredse og effektive gennem en oplevelse af en bedre og mere gnidningsfri løsning af deres opgaver på tværs af organisationer og sektorer.
2. **Borgernes** privatliv beskyttes gennem at indhente og udveksle så lidt information som muligt ud fra princippet om dataminimering.

3. For at højne sikkerhed, privatliv og tillid for **medarbejdere samt borgere**, har tjenesteudbyder dataansvaret og dermed det juridiske ansvar - her at viden om konsekvenser ved tildeling af adgange.
4. Brugerstyring adskilles fra it-fagløsninger for at opnå større sikkerhed og for at opnå større brugervenlighed **for borgere og medarbejdere**. Ligeledes understøtter det effektivisering af brugeradministrationen for medarbejdere.
5. **Medarbejdere og borgere** vil opleve effektive og opdaterede løsninger grundet løst koblede løsninger der bygger på standarder.
6. It-løsninger indgår i formelle samarbejder (føderationer) hvor spillereglerne er entydige, hvilket løfter sikkerhed og kvalitet på tværs af løsninger til gavn for **medarbejdere og borgere**.

De fælleskommunale arkitekturmål samt referencearkitekturen for brugerstyring giver nogle overordnede rammer og retning, men på løsningsniveau er det i høj grad op til de enkelte projekter, hvilken form for brugerstyring de vælger med konsekvenser for samspillet med de øvrige myndigheder.

På det mere tekniske plan har vi desuden 'KL's Anbefalinger om tekniske minimumskrav i kommunerne 2023', som

Bilag

De fælleskommunale arkitekturmål, vedtaget af KL's bestyrelse 2018:
Fælleskommunale arkitekturmål (kl.dk)
Referencearkitektur for brugerstyring v. 1.1 – Fælles Digital Arkitektur
Introduktion til referencearkitektur for brugerstyring | Fællesoffentlig Digital Arkitektur (digst.dk)
Anbefalingerne til tekniske minimumsstandarder – KL, 2023

3.3. Potentialer ved et målbillede for sammenhængende brugerstyring på det kommunale område

SAG-2023-03577 Jakob Eiby og Peter Falkenberg

Baggrund

Når kommunale medarbejdere bruger it-systemer i hverdagen, logger de på via en brugerstyringsløsning. Den lokale brugerstyringsløsning giver adgang til lokale systemer, Fælleskommunal Adgangsstyring giver adgang til KOMBITs løsninger og den fælleskommunale infrastruktur, og fx MitID Erhverv eller Sundhedsvæsenets Elektroniske Brugerstyring (SEB) giver adgang til fælles løsninger på tværoffentlige områder som fx sundhed eller miljø.

I Danmark er der på tværs af sektorer og fagområder etableret en række brugerstyringsløsninger – såkaldte *føderationer* – der sænker barren for at

udbyde og anvende tjenester for tjenesteudbydere og kommuner inden for den enkelte føderation ved at udstille disse fælles tjenester til brugerstyring.

Kommunerne oplever imidlertid et stigende behov for adgang på tværs af de forskellige områder, så brugervenligheden øges for medarbejderne, potentialer og besparelser ved de eksisterende standarder og brugerstyringsløsninger realiseres, og sikkerheden øges på tværs til gavn for borgerne.

På sundhedsområdet har man fx beskrevet et målbillede for sammenhængende brugerstyring (se bilag), der skal understøtte, at man bygger bro mellem de sektor- og fagspecifikke brugerstyringsløsninger.

KL vurderer, at et tilsvarende målbillede kunne danne rammen for det videre arbejde med sammenhængende brugerstyring på det kommunale område.

Indstilling
Sekretariatet indstiller, at It-Arkitekturrådet:

- Drøfter elementer i et eventuelt målbillede for brugerstyring

Sagsfremstilling
Rammearkitekturens sikkerhedsmodel handler om at styre, hvilke brugere og systemer, der får adgang til it-systemer. Adgangsstyring for brugere håndterer både, hvilke medarbejdere der kan logge ind i et it-system, og hvilken adgang medarbejderne får til it-systemets data og funktionalitet.1

Fælleskommunal Adgangsstyring for brugere er baseret på:

1) en *fødereret* model, der betyder, at brugere oprettes, tildeles adgang og autentificeres lokalt hos de enkelte kommuner;
2) fællesoffentlige standarder i overensstemmelse med princip 8 for Rammearkitekturens sikkerhedsmodel,2 så det bliver muligt at *føderere* med brugerstyringsløsninger på andre områder.

Fælleskommunal Adgangsstyring er udviklet i overensstemmelse med princip 4 i fællesoffentlig referencearkitektur for brugerstyring, der anbefaler, at "brugerstyring er adskilt fra forretningstjenesterhttps://arkitektur.digst.dk/node/1098 - princip-6-tjenesteudbydere-indg-r-i-f-derationer", og at etablering af brugerstyring i en

1 Vilkår for anvendelse af sikkerhedsmodellen i den fælleskommunale Rammearkitektur s. 3.

2 Beskrivelse af sikkerhedsmodellen i Rammearkitekturen s. 4.

selvstændig løsning er en forudsætning for, at medarbejdere kan opleve *sammenhængende, effektive og sikre* forløb på tværs af systemer.

Det sikrer sikkerhed, privatliv og tillid, sammenhæng og effektivitet, fordi:

- Det giver større brugervenlighed, når samme digitale identitet kan benyttes til flere tjenester, med mulighed for adgangsstyring på tværs af løsninger og domæner.
- Brugeradministrationen effektiviseres, idet brugerne ikke skal vedligeholdes flere steder og det øger sandsynligheden for korrekt oprydning i brugere og rettigheder.
- Det giver mindre overlap og dublering, når brugerstyring kan anvendes til mange tjenester, hvilket sparer penge ved udvikling og drift af applikationerne og resulterer i mere effektive løsninger.
- Sikkerheden øges når brugerstyring foregår i dedikerede tjenester, hvor fokus er på brugerstyring.

Anbefalinger om tekniske minimumskrav i kommunerne 2023

Formålet med anbefalingerne er at lette opgaven i den enkelte kommune med at vurdere, hvad der er et tilstrækkeligt minimumsniveau for sikkerhed i det tekniske udstyr og at understøtte god beskyttelse af it-udstyr og netværk mod hackerangreb og malware. Og dermed at beskytte medarbejdere og borgeres oplysninger mod at blive kompromitteret eller misbrugt.

Anbefalingerne er udarbejdet af KL i samarbejde med en række kommuner og tager afsæt i vejledninger fra Digitaliseringsstyrelsen, Center for Cybersikkerhed og Datatilsynet eller er udtryk for alment anerkendt best practice.

Det drejer sig bl.a. om følgende anbefalinger, der er relevante for brugerstyring i kommunerne:

- S6: Administrative rettigheder for brugere tildeles kun tidsbegrænset og med veldokumenterede behov.
- S10: Autentifikation til kommunens systemer over internettet skal anvende to-faktorlogin.
- S11: Alle platforme, hvor man logger på med kommunens loginmidler, må kun anvendes udenfor kommunens lokale netværk, hvis dette foregår vha. to-faktorlogin eller via en krypteret forbindelse til kommunens netværk.
- K7: Der skal være adgangskontrol for fysisk adgang til rum med følsomme oplysninger eller udstyr såsom servere, netværksudstyr, der håndterer intern trafik mv.
- K8: Ekstern adgang til fx konsulenter skal tildeles tidsbegrænset og kun til og med opgavens ophør. Den eksterne adgang skal kun

inkludere adgang til relevante systemer til den konkrete opgaveløsning.
- K9: Passwords skal udformes, opdateres og opbevares i overensstemmelse med Center for Cybersikkerheds anbefalinger.

Anbefalingerne skal understøtte, at kommunerne opnår en mere sammenhængende brugerstyring med de gevinster, det indebærer.

Potentiale ved et fælles målbillede
Vi har ikke et fælles målbillede på sammenhængende brugerstyring på det kommunale område, og derfor risikerer kommunerne at gå glip af nogle af de potentielle gevinster, der kan realiseres med de eksisterende brugerstyringsløsninger, som vi har investeret i sammen, herunder større brugervenlighed for medarbejdere, mere effektive arbejdsgange for administration af brugere og rettigheder, øget sikkerhed og billigere vedligeholdelse og drift.

Med et fælles målbillede bliver KL og KOMBIT meget bedre rustet til at varetage kommunernes interesser over for andre offentlige og private aktører og samtidig håndtere de udfordringer, der dukker op, og det stigende behov for mere sammenhængende brugerstyring på det kommunale område. Samtidig får kommunerne et fælles udgangspunkt for at stille krav til leverandørerne.

I første omgang er der behov for at etablere fælleskommunal enighed om en vision for et sammenhængende økosystem for brugerstyring med afsæt i eksisterende rammer og løsninger. Det vil derfor være nødvendigt at tage et bredt afsæt i relation til det nuværende it-landskab, herunder fælleskommunale platforme/komponenter som Danmark Miljøportal, National Sundhedsplatform, Unilogin mv.
Visionen bør dernæst konkretiseres med brugsscenarier i en sådan grad at det bliver muligt for de forskellige aktører at handle i overensstemmelse med målbilledet. En sådan indsats vil kræve bred kommunal forankring.

Bilag
Målbillede for sammenhængende brugerstyring version 1.1.1 (2020)
Anbefalingerne til tekniske minimumsstandarder – KL 2023

3.4. Status og videreudvikling af Fælleskommunal Adgangsstyring

SAG-2023-03577 Rasmus Halkjær og Jakob Eiby

Baggrund
Sagen indeholder en status for implementering af NSIS og en række mindre tiltag i en version 2 af Fælleskommunal Adgangsstyring (FK-A) for brugere og systemer, samt et roadmap for en videreudvikling, der gør løsningen nemmere at anvende for kommuner og leverandører, der ønsker at koble sig til.

Indstilling
Sekretariatet indstiller, at It-Arkitekturrådet:

- tager status til efterretning
- giver input til den videre udvikling af Fælleskommunal Adgangsstyring, herunder til, hvad der skal til for øge anvendelsen

Sagsfremstilling
KOMBIT har videreudviklet Fælleskommunal Adgangsstyring for brugere (Context Handler) og systemer (Security Token Service) med henblik på 1) at understøtte NSIS for brugere og 2) indføre ny funktionalitet for systemer.

<u>Implementering:</u>
Kommunerne og KOMBIT har følgende hovedopgaver efter den nye Context Handler 2 (CH2) og Security Token Service 2 (STS2) er i produktion:

- Kommuner skal etablere tillid til CH2 i deres lokale brugerstyringsløsning (også kaldt lokal IdP)
  - Det er gennemført for samtlige kommuner i produktion
- Kommuner skal teste integrationen i test og produktion
  - Det er gennemført for samtlige kommuner i produktion
  - Tre kommuner skal dog lave step-up med MitID erhverv, forventes gennemført efter den 04-04-2024
- KOMBIT skal teste føderation med sundhedsområdets brugerstyringsløsning (SEB)
  - Føderationstest er gennemført med Københavns Kommune og Sundhedsdatastyrelsen (SDS)
  - Der mangler fastlæggelse af dato for, hvornår det implementeres i produktion, da det kommer an på, hvornår kommunerne kan levere et NSIS-sikringsniveau på ’betydelig’, enten via egen IdP eller via MitID erhverv
- KOMBIT skal planlægge de fælleskommunale løsningers overgang til CH2 og STS2, særligt med hensyn til softwarerobotter

<u>Videreudvikling af Fælleskommunal Adgangsstyring</u>

Følgende er et overblik over udviklingsaktiviteter, afklaringer og boblere.

Under udvikling:

- CR287 OIOSAML Profiler og VA319 NSIS i Relaystate RPA (robotter på CH2)
    - Dette er en kombination af to ændringsanmodninger der sammen løser to hovedproblemstillinger:
        1. Give kommunerne større fleksibilitet i understøttelse af robotter med NIST-sikringsniveauer
        2. Hvordan skal det krævede NSIS sikringsniveauer kommunikeres fra CH2 til kommunens IDP
- VA326 Tillæg til ADG2 attributservice
    - For at Københavns Kommune kan få deres brugere på i de tilfælde, hvor rettigheder fylder mere end 10kb
- VA-311 - NSIS Revisionserklæring - Design og implementering
    - Den årlige NSIS-revisionserklæring for CH2
- VA-310 CH - OIDC Auth Server
    - Understøttelse til Mobile og Tablets
      Uddybet yderligere under punktet *Open ID Connect
- VA-321 IDWS referenceimplementering cert opdatering
    - Opdatering af certifikater på IDWS referenceimplementering til anvendersystemers anvendelse af tokenbeskyttede services der anvender OIOIDWS binding 1.2

Følgende punkter er under afklaring og men ikke lavet som ændringsanmodning endnu:

- Robotter under NSIS
    - Under afklaring med DIGST og KL
      Uddybet yderligere under **Konsekvenser for kommunernes brug af softwarerobotter
- Opgradering af fælleskommunale attributprofiler
    - CH2 kan med en lille udvidelse arbejde med dynamiske attributprofiler. Dvs at brugervendte systemer selv bestemmer, hvad de vil modtage fra kommunens IdP
      Problemet er, hvordan vi får kommunikeret nye attributter til kommunernes IdP'er, og hvordan de administreres
- NIS2
    - I gang med at undersøge om CH2/STS2 skal overholde NIS2, samt hvem der eventuelt skal betale

Boblere:

- Relationship-based access control (ReBAC) i kommunal adgangsstyring
- View my token - Hjælpeværktøjer til at teste log-in
- Open ID Connect – IdP del

- Forbedring af Fejlmeddelser fra CH 2
- Overvågning af fejl og opfølgning med anvendere
- AI til loganalyse – Strategi og afklaring
- Borger token / IDWS-understøttelse (skal ikke forveksles med IDWS binding)

*Open ID Connect (OIDC)
Context Handler 2 udstiller en service til autentifikation og autorisation, baseret på en profilering af den fællesoffentlige sikkerhedsstandard OIOSAML.

Det har sikret medarbejdere ét fælles login (*single sign on*) på det kommunale område, og skaber tilmed sammenhæng til andre brugerstyringsløsninger, fx NemLog-in og Sundhedsvæsenets Elektroniske Brugerstyring (SEB).

Kommunerne og leverandørerne har gennem mange år efterspurgt en nemmere understøttelse af simple applikationer og mobilapps, så det bliver nemmere at koble nye løsninger på den fælles brugerstyringsløsning, og så løsningen:
- giver samme niveau af sikkerhed ved autentifikation (login)
- ikke behøver at give samme muligheder for en uddybet autorisationsdel

For at understøtte simple applikationer og mobilapps bedre og gøre det nemmere for kommuner og leverandører at anvende Fælleskommunal Adgangsstyring, vil CH2 udvikle muligheden for at udstille både de eksisterende OIOSAML-services og nye OIDC-services. Begge dele baserer sig fortsat på kommunernes rolle- og rettighedstildelinger via deres lokale brugerstyringsløsninger.

Den anden del af OIDC, der taler sammen med kommunernes brugerstyringsløsninger, er ikke planlagt endnu, da man fortsat baserer sig på SAML.

**Konsekvenser for kommunernes brug af softwarerobotter
Overgangen til NSIS via CH2 udfordrer den kommunale praksis med brug af softwarerobotter, hvis KOMBITs eller andre fælles løsninger stiller krav om brug af NSIS. Det skyldes, at NSIS regulerer sikkerheden for *person*brugere, og derfor ikke kan bruges til at stille sikkerhed for *robot*brugere.

KL og KOMBIT arbejder derfor på at samle kommunerne og træffe en strategisk beslutning om implementering af NSIS i KOMBITs systemer og et

fælles udgangspunkt og roadmap for fremtidig håndtering af softwarerobotter.

I forlængelse af ovenstående beslutning skal kommunerne tage stilling til, hvordan KL og KOMBIT bør forsøge at påvirke andre offentlige myndigheder, fx Politiet, der ikke vil have brugergrænsefladerobotter i deres løsninger og ikke har – eller har tænkt sig at tilvejebringe – brugbare alternativer.

Større udnyttelse af Fælleskommunal Adgangsstyring
For at øge udnyttelsen af FK-A har KOMBIT gennem de sidste år iværksat en række kommune- og leverandørrettede initiativer, og KOMBIT opgør løbende graden af anvendelse. Udnyttelsesgraden fremgår af 'Infrastrukturen i tal' (et Power BI-baseret dataværktøj) jf bilag.

KOMBIT udarbejder desuden 'FKI Potentiale', jf bilag, hvor kommunerne kan se hvilke integrationspakker og integrationer i den fælleskommunale infrastruktur, der er relevant for det enkelte specifikke it-system. FKI Potentiale omfatter endvidere nøgletal for it-systemernes tilslutning, kommunernes ibrugtagning og samlet målopfyldelse for udbredelsen af den fælleskommunale infrastruktur. Nøgletallene opdateres en gang om måneden.

KOMBIT gennemfører aktuelt en kortlægning af, om kommunerne anvender eller ikke anvender it-systemer der kan tilføjes i 'FKI Potentiale'. Denne kortlægning vil foreligge til mødet 24. april.

På mødet fremlægges en kommunal case om erfaringer med at få koblet flere løsninger på FK-A, herunder de barrierer kommunen oplever i den forbindelse.

Bilag
De kommunale systemers anvendelse af FK-A i Infrastrukturen i tal.
FKI Potentialerapport: Infrastrukturen i tal | Digitaliseringskataloget

3.5. Afgrænsning af data og brugeradgange - Status for dataafgrænsningsanalysen

SAG-2023-03577 Mette Jespersen

Baggrund

Aalborg Kommune og Favrskov Kommune har i 2022 over for KOMBIT og KL rejst en problemstilling vedr. dataafgrænsning med de fælleskommunale værktøjer, relateret til tværgående adgangsgrupper og/eller midlertidige grupperinger af medarbejdere.

På baggrund af henvendelsen igangsatte den kommunale styregruppe for Den fælleskommunale infrastruktur (FKI) sammen med SAPA-projektet en analyse af en række kommuners udfordringer med at begrænse medarbejdernes adgang til borgernes data.

Indstilling
Sekretariatet indstiller, at It-Arkitekturrådet:

- kommer med input til analysen og det videre forløb

Sagsfremstilling
En arbejdsgruppe i KOMBIT-regi fik i 2023 til opgave at gennemføre en analyse af behov for udvidede muligheder for dataafgrænsning i den fælleskommunale infrastruktur.
I arbejdsgruppen indgår foruden KOMBIT, KL, Aalborg Kommune, Favrskov Kommune, Holstebro Kommune, Odense Kommune, Næstved Kommune og Skanderborg Kommune.

Arbejdsgruppen har kortlagt udfordringerne med ophæng til FKI og SAPA kommunestyregrupper og har identificeret følgende problemstillinger:

- **Tværorganisatoriske teams**
  Dataafgrænsning på mindre teams på tværs af organisationen og KLE
- **Adgang for alle**
  Dataafgrænsning af sager inden for et KLE-emne, som alle medarbejdere må tilgå
- **Detaljering af organisationsstrukturen**
  Dataafgrænsning på mindre teams, som ikke fremgår af den administrative organisationsstruktur
- **Dataafgrænsning ud fra ansættelsessted**
  Dataafgrænsning hvis medarbejderen har flere ansættelser i kommunen
- **Monopolisering af KLE-emner i FK Organisation**
  Dataafgrænsning med KLE-emner, hvis et fagsystem stiller særlig krav til opmærkningen med KLE

Arbejdsgruppen drøfter den 10. april udfordringerne på en halvdagsworkshop. På Arkitekturrådets møde 24. april vil arbejdsgruppen fremlægge resultater fra workshoppen samt plan for det videre arbejde med ovenstående problemstillinger.

Bilag
Dataafgrænsning - Scope for analyse af den nødvendige og relevante dataafgrænsning i den fælleskommunale infrastruktur, version 0.3. KOMBIT, december 2022.

3.6. Potentialer ved automatisering og optimering af brugerstyring og onboardingprocesser i kommunerne

SAG-2023-03577 Vibeke Normann

Baggrund
I regi af 10-årsplanen for ny teknologi og automatisering af den offentlige sektor, som er et samarbejde mellem Stat, regioner og kommuner om at frigøre 10.000 arbejdspladser inden 2030, har KL fået udarbejdet en analyse af potentialerne ved automatisering og optimering af brugerstyring.

Indstilling
Sekretariatet indstiller, at It-Arkitekturrådet:

- Drøfter de forslag til implementeringsinitiativer, som indgår i analysen 'Automatisering og optimering af brugerstyring og onboardingprocesser i kommunerne'
- Giver input til den eventuelle videre proces

Sagsfremstilling
I sin analyse 'Automatisering og optimering af brugerstyring og onboardingprocesser i kommunerne' foreslår PwC en række implementeringsinitiativer.
Initiativerne bygger på tre kommunale arketyper, som hver især repræsenterer et vist modenhedsniveau, beskrevet ud fra fem områder: Ledelse, Processer, Kompetencer, It-understøttelse og Integrationer.

Det drejer sig om følgende forslag til initiativer:

1. Etablering af fundament for ledelsesstøtte til IdM

2. Fælleskommunal rollebeskrivelse af jobfunktioner og standardisering af begreber
3. Model for tilslutning af applikationer og systemer
4. IdM strategi, kapabilitetskortlægning og driftsmodel
5. Fælleskommunale netværk
6. Standardiserede IdM-løsninger
7. Styrke FKI og anvendelsen i leverandørernes it-systemer
8. Fælles og standardiseret IdM-arkitektur
9. End-to-End proces og datamodel

Initiativerne kan gennemføres enten fælleskommunalt eller individuelt i kommunerne, og analysen estimerer, at initiativerne samlet har et årligt potentiale på i alt cirka 240 årsværk.

KL vil med udgangspunkt i kommunernes ønsker og efterspørgsel forsøge at iværksætte en fælleskommunal indsats om brugerstyring og onboarding.

På mødet præsenterer PwC de væsentligste pointer i analysen med fokus på forslagene til implementeringsinitiativer.

Bilag
'Automatisering og optimering af brugerstyring og onboardingsprocesser i kommunerne', PwC februar 2024
'Automatisering og optimering af brugerstyring og onboardingsprocesser i kommunerne' - Ledelsesresumé, PwC februar 2024

4. Eventuelt