



Rettighedsstyring for eksterne brugere – Diskussion af scenarier

Kolofon:

OIO Referencemodel for tværgående brugerstyring

Dette diskussionspapir kan frit anvendes af alle. Citeres fra dokumentet i andre publikationer til offentligheden skal angives korrekt kildehenvisning.

Forslag til anbefalinger for tværgående brugerstyring udarbejdes af IT- og Telestyrelsen, IT-strategisk kontor, som sekretariat for OIO It-Arkitekturkomiteen.

Kontaktperson:

It-Arkitekt Søren Peter Nielsen, email: spn@itst.dk

Telefon 25 67 07 83 (direkte)

It-Arkitekt Anders Dalsgaard, email: ada@itst.dk

Telefon 25 65 32 08 (direkte)

Ministeriet for Videnskab, Teknologi og Udvikling

IT- og Telestyrelsen

IT-strategisk kontor

Holsteinsgade 63

DK-2100 København Ø

Telf. +45 35 45 00 00

Fax. +45 35 45 00 10

<http://www.itst.dk>

itst@itst.dk

Indholdsfortegnelse

1	Introduktion	4
1.1	Baggrund.....	4
1.2	Formål	5
1.3	Antagelser	5
1.4	Fire overordnede scenarier.....	5
2	Central administration	6
3	Decentral administration	7
4	Forvaltningsfællesskab	8
5	Logning og kontrol	9
6	Diskussion	10
6.1	Standarder til synkronisering af brugerinformation mellem brugerkataloger.....	12
6.2	Unik repræsentation af ressourcer.....	13
6.3	Synkronisering af ressource-beskyttelse-information	14
7	Videre arbejde	14
8	Appendiks A - Definitioner	15
9	Appendiks B - Yderligere information	15

1 Introduktion

Dette dokument gennemgår forskellige scenarier for styring af eksterne brugeres rettigheder i forbindelse med digital forvaltning. Fordele og ulemper ved de forskellige scenarier diskuteres, men der konkluderes ikke til fordel for et specifikt scenarium i dette dokument, dels fordi der forventes en situation, som er en kombination af flere forskellige scenarier, dels fordi det forventes, at anvendelsen af forskellige scenarier vil gennemgå naturlige skift efterhånden som det tekniske og organisatoriske grundlag for digital forvaltning udvikler sig.

Vi forventer således, at flere forskellige modeller for håndtering af eksterne brugeres rettigheder vil komme i anvendelse på forskellige stadier af udviklingen i digital forvaltning. Disse modeller inkluderer to væsentligt forskellige tilgangsmåder.

I den første tilgangsmåde administreres eksterne brugeres rettigheder af en lokal administrator i egen organisation. I denne tilgang kan der ske en udvikling fra manuel administration over til administration i eget lokale rettighedssystem og efterfølgende udveksling med rettighedssystemet for den givne løsning, og slutteligt til en situation hvor der er udviklet et *fælles sprog* for rettighedstildeling inden for digital forvaltning. Her tildeles brugere dynamisk rettigheder på baggrund af den basis-information der medfølger om dem. For denne tilgangsmåde diskuteres hvilke standarder, der kan anvendes til at skabe en fælles tilgang til løsningerne til trods for anvendelse af forskellige modeller for håndtering af eksterne brugere.

I den anden tilgangsmåde sker styring af rettigheder via uddannelse og information til brugerne, således at de ved, hvilke rettigheder og pligter, de har som følge af deres jobfunktion eller rolle. I det tilfælde sker der ingen teknisk håndhævelse af rettighedsbegrænsninger, men der sker en logning af alle kritiske handlinger. Her kan det forventes, at udviklingen går fra traditionel logning og kontrol af stikprøvekontroller i logfilerne, over til automatisk hjælp til kontrollen vha. søgning i logfiler efter specielle mønstre, afvigelser etc. – og videre til en situation, hvor kontrollen sker proaktivt i realtid. Dette giver fx mulighed for, at der kan gives advarsler om brugsmønstre, som peger på uberettiget brug af en given løsning. Der diskuteres ikke mulige standarder for denne tilgangsmåde i den nuværende version af dokumentet.

1.1 Baggrund

I forbindelse med implementeringen af digital forvaltning i Danmark er der voksende behov for, at de offentlige digitale løsninger skal kunne håndtere brugere¹, der ikke har deres primære forankring i den samme organisation, som ejer løsningen. Behovet for at kunne håndtere eksterne brugere er afledt af følgende overordnede behov i forbindelse med digital forvaltning:

- Interoperabilitet
- Samarbejde (Collaboration)
- Nytænkning af måden offentlige ydelser leveres på (Transformation)

Disse tre overordnede behov bygger i høj grad på hinanden – det vil sige: Interoperabilitet er i høj grad en forudsætning for samarbejde (Collaboration), og nytænkning i måden at levere offentlige ydelser på forudsætter også en høj grad af interoperabilitet samt samarbejde².

Dette dokument diskuterer forskellige måder, som offentlige organisationer kan vælge at håndtere problematikken med eksterne brugere på i forhold til de krav som interoperabilitet, samarbejde og nytænkning stiller til styring og kontrol af eksterne brugeres rettigheder.

Dokumentet er altså et diskussionsoplæg om, hvorledes information om eksterne brugeres rettigheder administreres, udveksles, samt hvorledes det kontrolleres, at ønskelig adfærd udvises.

¹ Med brugere menes både borgere såvel som ansatte i andre offentlige organisation og private virksomheder.

² En engelsk definition af begreberne interoperability, collaboration og business transformation findes i Appendiks.

1.2 Formål

Formålet med høringen af dette dokument er, at modtage tilbagemeldinger på de diskuterede scenarier og tendenser. På basis af tilbagemeldingerne er det planen, at en opdateret udgave af diskussionspapiret publiceres, så det kan indgå som baggrundsmateriale for fremtidige overvejelser om tværgående rettighedsstyring i offentlige it-systemer.

1.3 Antagelser

Vi antager, at de involverede organisationer er enige om, hvorledes brugers identitet fastslås, og hvorledes information om en brugers identitet udveksles. Dokumentet beskæftiger sig altså ikke med disse problemstillinger, men forudsætter dem løst. Følgende dokumenter, som er i høring samtidigt med dette dokument, indeholder anbefalinger til understøttelse af tværgående udveksling af information om en brugers identitet:

- Vejledning vedrørende niveauer af autenticitetssikring
- Anbefaling om fælles arkitektur for tværgående autenticitetssikring
- Anbefaling til kerneattributter for bruger
- Anbefaling til unik id-nøgle

Vi antager også, at mekanismen til udveksling af information om en brugers identitet også kan anvendes til at udveksle information om en brugers rettigheder. Standarden SAML 2.0 har status anbefalet i OIO-kataloget over offentlige it-standarder og understøtter en sådan mekanisme. Vor anbefaling er, at SAML anvendes til udveksling af information om brugerens identitet. Rettighedsinformation kan, som vi senere diskuterer, være angivet i standarden XACML, der også kan udveksles via SAML.

En ekstern bruger kan være en borger såvel som en ansat i offentlig eller privat virksomhed. Diskussionerne i dokumentet har dog mest fokus på ansatte i virksomheder, som typisk skal tildeles en række differentierede rettigheder. Rettighedsstyring for borgere generelt er mere simpel. Enten skal en borger have adgang til samme ressourcer som alle andre borgere, eller også skal borgeren have adgang til ressourcer og informationer, som specifikt har med borgerens forhold at gøre. Endelig er en tredje mulighed at borgerens rettigheder skal delegeres til anden bruger, men der er stadig tale om en relativt simpel situation i forhold til rettighedstildeling til forskellige jobfunktioner og roller, som ansatte kan have.

1.4 Fire overordnede scenarier

I det følgende beskriver vi kort fire overordnede scenarier og går derefter mere i detaljer med et par af dem. De fire scenarier har vi benævnt således:

- Central administration
- Decentral administration
- Forvaltningsfællesskab
- Logning og kontrol

Fordele og ulemper ved de forskellige scenarier diskuteres. Det er vigtigt at holde sig for øje, at selvom der er løsninger for digitalt forvaltning, som måske ikke ser ud til at være generelt holdbare på sigt, kan de være det bedste valg inden for givne løsningsområder med de begrænsninger, der findes i dag. Det er altså også et spørgsmål om at identificere hvilke modeller, vi kan få til at virke i dag, og hvorledes vi kan udbygge dem således, at de kan "vokse" til at blive mere generelt anvendelige til digitalt forvaltning.

Scenarierne er skitseret ud fra problemstillingen for en given organisation, som skal give eksterne brugere adgang til en eller flere løsninger, som man er ansvarlige for. Man kan sige, at vi anskuer udfordringen fra applikationsejerens synspunkt. Det er vigtigt at bemærke, at en given "ekstern bruger" vil have behov for

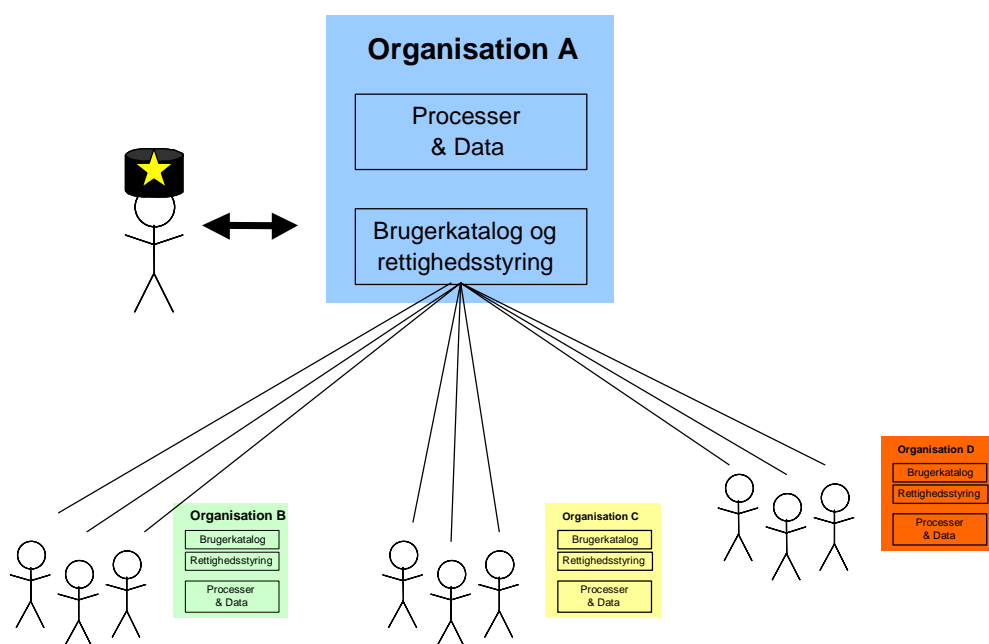
rettigheder til flere forskellige løsninger, som forskellige organisationer har ansvaret for. Der er altså også behov for at overveje, hvilke udfordringer (blandt andet administrative) der er for de eksterne brugeres organisationer. En væsentlig udfordring er at finde løsninger som kan skaleres op til at favne alle disse forskellige – og måske interrelaterede – behov.

De forskellige scenarier for håndtering af eksterne brugeres rettigheder beskrives de følgende kapitler.

Det skal her noteres, at selvom 'Logning og Kontrol' er et selvstændigt scenarie, indgår logning og kontrol i hvert af de øvrige scenarier som et ekstra sikkerhedslag og kan ikke udelades.

2 Central administration

I dette scenarium er det en central instans eller organisationen, der har ansvaret for oprettelse af og tildeling af rettigheder til eksterne brugere for en given løsning. Dette er illustreret i den følgende figur:



Fordele

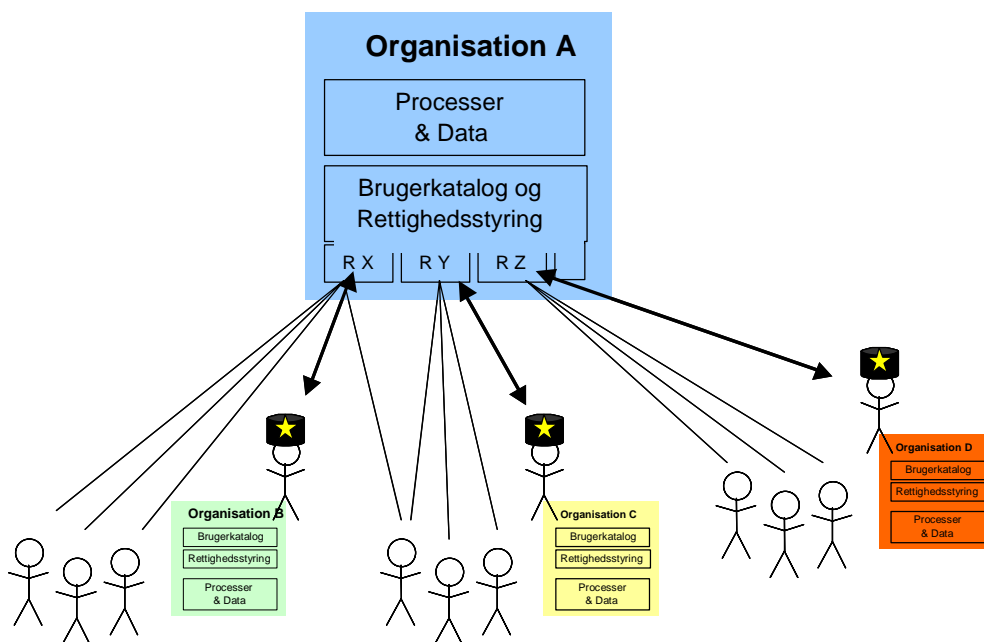
- Den centrale administrator har mulighed for at kende løsningen godt, og har dermed mulighed for godt kendskab til, hvor meget en given ekstern bruger rent faktisk får adgang til på de forskellige rettighedsniveauer i løsningen.
- Stor trykthed for deltagende organisationer, da ansvaret er placeret hos én organisation, som har fuld kontrol.
- Der kan muligvis stilles færre tekniske krav til interoperabilitet vedrørende brugerrettighedsoplysninger, hvis den væsentligste del af administrationsarbejdet sker inden for én organisation.
- Det er nemmere at holde styr på oprydning af inaktive brugere etc. – hvilket ofte er et problem for decentrale løsninger.

Ulemper

- Den centrale administrator skal have mange informationer om hver enkelt ekstern bruger – samt indsigt i arbejdsprocesserne i de organisationer som de eksterne brugere er ansat i for at kunne vurdere, hvilke rettigheder de skal tildeles.
- Der skal etableres processer til notifikation om ændringer i brugerstatus (ansættelse, ændring i jobrolle, afsked, etc.) for alle organisationer, hvori der sidder eksterne brugere.
- Stor administrativ byrde for den centrale organisation, som ikke umiddelbart er værdibringende. Fordeling af brugeradministrationsudgiften på de eksterne organisationer medfører yderligere administration – og evt. ønske fra de eksterne organisationer om at ”hjemtage” brugeradministrationsopgaven.

3 Decentral administration

I scenariet med decentral administration er det stadig organisationen, der har ansvaret for en given løsning, som bestemmer hvilke brugere, der må få hvilke adgangsniveauer. Dette antages løst ved, at organisationen tilknytter sine rettigheder (eller privilegier) til en række roller. Således kan en bruger tildeles en række rettigheder ved blot at få en rolle tilknyttet. Roller er også relevante for scenariet med central administration. Imidlertid håndteres tildelingen af roller til eksterne brugere i dette scenarium af lokale administratorer hos de eksterne organisationer, der tilgår løsningen. Dette er illustreret i følgende figur



En given organisations lokale administrator kan også give rettigheder til 3. mand – fx revisor – som må agere på organisationens vegne inden for et afgrænset område.

Fordele

- Den lokale administrator har bedre indsigt i, hvilke adgangsrettigheder brugerne skal have for at kunne udføre deres job.
- At opgaven med oprettelse, ændring og nedlæggelse af brugere er lokal giver større sandsynlighed for at de eksterne brugeres rettighedstildeling er korrekt, end hvis det skal håndteres af én central funktion.

- Den administrative byrde spredes ud til de organisationer, der nyder godt af adgangen til løsningen – og muliggør indarbejdelse i de øvrige brugerstyrings-administrative procedurer i de enkelte organisationer.

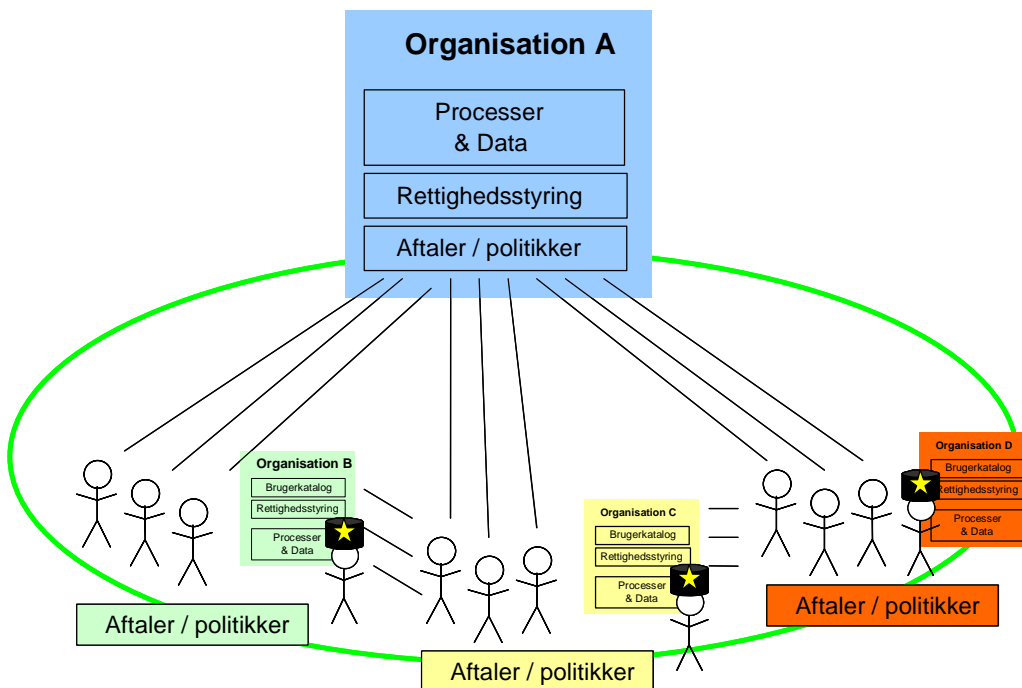
Ulemper

- Modellen er rettet mod centrale løsninger, som der kun er én af inden for universet for digital forvaltning (som fx ToldSkat's skatteløsninger). Ved behov for tilgang til mange forskellige løsninger hos forskellige organisationer (som fx inden for sundhedsvæsenet) er der fare for, at den administrative byrde hos den enkelte organisation med eksterne brugere vokser kraftigt.
- Oprydning af inaktive brugere er en stor udfordring ved decentral administration, såfremt det er en manuel opgave for lokale administratører at foretage denne oprydning.

Styring af rettigheder i forbindelse med Virk.dk og Nemkonto er eksempler på decentral administration, hvor der udnævnes en lokal administrator for hver ekstern organisation, som så tildeler rettigheder til egne brugere og 3. parter, som agerer på organisationens vegne.

4 Forvaltningsfællesskab

Dette scenarium beskriver, hvorledes eksterne brugere dynamisk tildeles rettigheder til en given applikation på baggrund af information om dem, som "sendes med", eller som organisationen med løsningen allerede har skaffet til egne behov. Dette scenarium svarer mest til visionen om den fremtidige serviceorienterede arkitektur og beskrives blandt andet i dele af *Federation of Identities in a Web Services World - A Joint Whitepaper from IBM Corporation and Microsoft Corporation, Version 1.0, July 8, 2003*³. Med forvaltningsfællesskab er brugere i stand til at tilgå andre organisationers it-systemer uden at være registreret som bruger hos disse organisationer. Ligeledes kan brugere tildeles rettigheder dynamisk på baggrund af information om brugeren (attributter, som fx roller). En af forudsætningerne for dette scenarium er, at der er skabt en formaliseret form for tillid i form af aftaler og politikker mellem den involverede organisation, som illustreret i følgende figur



³ <http://www-128.ibm.com/developerworks/webservices/library/ws-fedworld/index.html>

Fordele

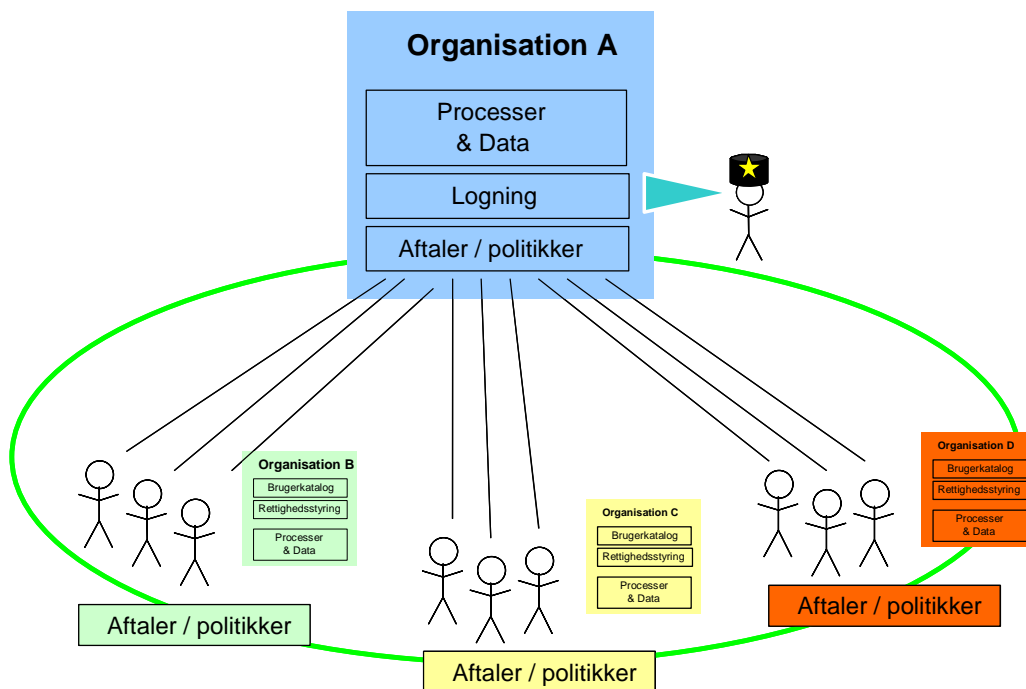
- Dynamisk tildeling af rettigheder sparer administrativt arbejde.
- Tilslutning af nye organisationer kræver ikke ændringer hos de bestående parter.

Ulemper

- Kræver etablering af tillid mellem organisationer på formel basis – dette er i dag stadig et område, der ikke er modent til generel anvendelse.
- Kræver ”fælles sprog” i beskrivelsen af brugernes attributter. Et sådant fælles sprog findes ikke inden for dansk digital forvaltning i dag - og skal først udvikles (kræver først, at de enkelte organisationer gennemgår en modning med hensyn til rolle-baseret adgangskontrol inden for egne løsninger).

5 Logning og kontrol

- I det fjerde scenarium er der ikke tale om begrænsning i rettigheder for eksterne brugere ved hjælp af tekniske foranstaltninger, men i stedet via uddannelse og information til brugerne, således at de ved, hvilke rettigheder de har som følge af deres rolle. Ved hjælp af effektiv logning og kontrol sikres, at der ikke sker misbrug i forbindelse med anvendelse af de givne løsninger. Dette scenarium er illustreret i den følgende figur.



Fordele

- Man vil ikke komme ud for situationer, hvor eksterne brugere ikke kan få adgang til nødvendige løsninger, blot fordi rettighedsstyringsinformationen ikke er opdateret – og der vil ikke opstå situationer, hvor en bruger ”låses ude” pga. en usædvanlig situation, som man ikke har forudset i sin rettighedstildeling.
- Løsningerne vil måske blive mindre komplekse, hvis der ikke behøves et rettighedsstyringsmodul.

Ulemper

- Det kan blive temmelig krævende at overbevise borgerne om, at data, som vedrører dem i løsninger uden tekniske foranstaltninger til adgangskontrol, håndteres på en ordentlig og sikker måde.
- Den nødvendige kontrol-opgave med inspektion af log-filerne kan blive en meget stor opgave
- Der er ingen modne standarder til understøttelse af logning og kontrol på tværs af organisationer
- Der er ingen almindeligt anvendt metode til beskrivelse af en bruger i en logfil, som gør det muligt at identificere brugeren unikt på tværs af systemer.

Anvendelse af dette scenarium uden kombination med andre tiltag er dog for nuværende kun en teoretisk mulighed. Bestemmelser i persondataloven og lov om patienters retsstilling tillader ikke en situation, hvor alle brugere uhindret har adgang til alle data inden for et område, der omfatter person/patient-følsomme informationer.

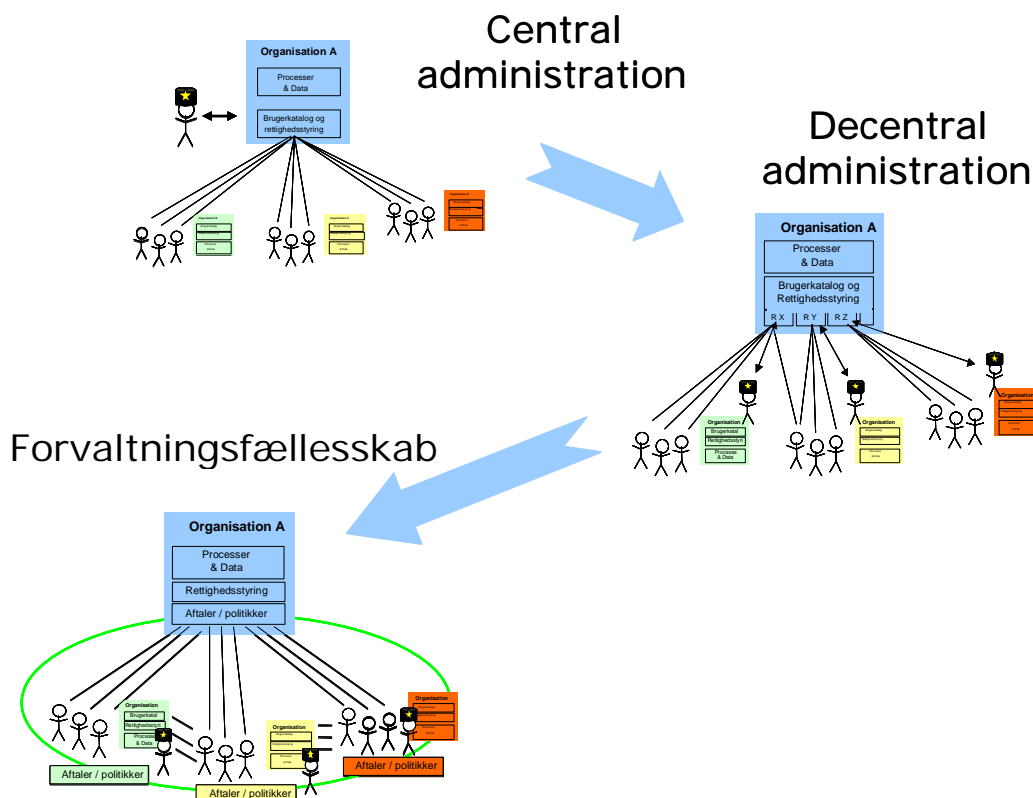
6 Diskussion

De fire scenarier, der er skitseret oven for, kan betragtes som forskellige valgmuligheder for en given opgave i dag. Men det er mere tanken, at de skal ses som muligheder, der vil skifte i relevans i takt med at digital forvaltning, og den tilhørende standardisering modnes og udbygges. Det må forventes, at flere af scenarierne vil komme i anvendelse på samme tid og skal kunne sameksistere.

Det ”rene” lognings- og kontrol-scenarium kan fx kombineres med løsninger, hvor der sker adgangsbegrænsning ved hjælp af tekniske foranstaltninger.

De tre andre scenarier afspejler mere en udvikling i mulighederne indenfor rettighedsstyring.

Udviklingen her forløber som illustreret nedenfor



Vi bevæger os mod en standardbaseret model med forvaltningsfællesskab fra et udgangspunkt, som i dag mest realistisk må betegnes som decentral administration. Central administration kan ikke skaleres op til at

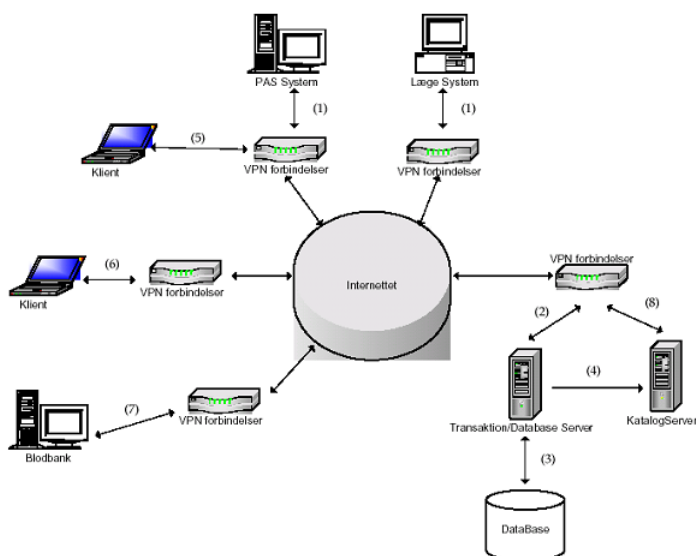
opfylde de behov, der er inden for digital forvaltning i dag vedrørende håndtering af eksterne brugere. Central administration kan således allerede betragtes som en model, der tilhører fortiden⁴. Samtidig stiller modellen med forvaltningsfællesskab nogle krav, som ikke kan indfries i dag. Det drejer sig både om organisatoriske krav (fx formel definition af tillid mellem organisationer), semantiske krav (fx fælles sprog for ”attributter”) og tekniske krav (fx modne federation-standarder).

Decentral administration ser ud til at være det mest realistiske valg for løsninger i dag, men decentral administration vil også give skaleringsudfordringer, efterhånden som interoperabiliteten i digital forvaltning udvikles. Det er derfor vigtigt, at løsninger med decentral administration designes således, at de er naturlige skridt på vejen mod modellen med forvaltningsfællesskab, og i overensstemmelse med fællesoffentlige it-standarder.

Fx vil løsninger med decentral administration, som kun giver adgang til at styre egne brugeres rettigheder manuelt (fx via web-browser), hurtigt blive en administrativ byrde for lokale administratorer, efterhånden som der kommer flere løsninger, hvor de skal styre egne brugeres rettigheder. Som et af de første skridt mod forvaltningsfællesskab må løsninger med decentral administration også kunne håndtere at bruger- og rettighedsoplysninger udveksles maskinelt.

Det er derfor en vigtig opgave at prøve at tegne de forskellige veje fremad og diskutere fordele og ulemper. Fx kan kravet fra det tidligere nævnte eksempel om, at administration af eksterne brugere skal kunne håndteres maskinelt, også foldes ud på forskellige måder.

Én tilgang er at en række af de løsninger, som har eksterne brugere går sammen om en fælles løsning til håndtering af eksterne brugere, således som fx skitseret i MedComs oplæg⁵ til brugerstyring inden for sundhedsdatanettet fra starten af 2003. Dette er illustreret i følgende figur.



I MedCom-oplægget opereres der med ét centralt bruger- og rettighedsstyringskatalog. Rettigheder tildeles i form af roller, som afhænger af hvilken organisation, man tilhører. I det konkrete eksempel er der forudsat etableringen af et fælles rollebegreb inden for den givne sektor. Dette er en antagelse, der ikke umiddelbart kan gøres generelt. Derudover kan det nævnes, at MedCom-oplægget har som fokus at styre *læse-adgange*

⁴ Centrale administrationsløsninger kan stadig være relevant i tilfælde, hvor brugerskaren er meget homogen til trods for, at den er spredt ud over mange organisationer, og hvor brugernes rettigheder kan angives på baggrund af generelle attributter, som fx niveau af faglig autorisation.

⁵ <http://www.medcom.dk/mc4/inet/tekn/bruger/index.htm>

for eksterne brugere. Hvis der også skal håndteres opdaterings-retteligheder for eksterne brugere, vil der være behov for yderligere granularitet i de retteligheder, som eksterne brugere skal kunne tilknyttes.

Et brugerkatalog, som samler alle brugere inden for et givent område, kan også medvirke til tværgående tjenester som instant messaging, virtuelle møder på en sikker måde, etc. Det skal bemærkes, at et centralt katalog kan blive single-point-of-failure for eksterne brugeres tilgang til et meget stort antal applikationer, hvorfor der vil være krav om en række tiltag til sikring af tilgængelighed, fx redundans i infrastrukturen.

En anden tilgang er, at den lokale administrator administrerer egne brugeres adgange til eksterne løsninger sammen med retteligheder til de interne løsninger. Denne tilgang kan fx udnytte provisionerings-løsninger⁶, der automatisk håndterer oprettelse, ændring og sletning af brugere. Når en provisioneringsløsning har oprettet en bruger i egen organisation, har vedkommende bruger også fået nødvendige retteligheder i eksterne løsninger, enten direkte via webservices eller ved definitioner i det lokale system og efterfølgende synkronisering.

Begge tilgange vil sikkert finde anvendelse. Det er her kritisk at sikre, at de to tilgangsmåder ikke udelukker hinanden. Dette sker ved at basere sig på standarder, fx vedrørende

- synkronisering af brugerinformation mellem brugerkataloger
- unik repræsentation af ressourcer som skal beskyttes
- synkronisering af ressource-beskyttelse-information

Vi vil kort diskutere standarder der er aktuelle i forhold til de ovennævnte punkter i dag.

6.1 Standarder til synkronisering af brugerinformation mellem brugerkataloger

Brugerkatalogerne, som skal synkroniseres, kan være LDAP-directories, relationelle databaser og eventuelt andre strukturer. Der kan også være modeller, som skitseret i MedCom-oplægget, hvor opdateringer og vedligehold sker i en relationel database, der synkroniseres med et LDAP-directory, som så anvendes til autenticitetssikring af de eksterne brugere. Anvendelsen af en relationel database giver fx også mulighed for at gemme ikke-katalogdata, og hele versionshistorien for ændringer i brugerkataloget.

Synkronisering af brugerinformation forudsætter enighed om, hvilke felter en bruger kan beskrives med, og hvilke der *skal* være udfyldt. Man skal være enige om den struktur (eller det *Schema*) som beskriver brugeren.

6.1.1 LDIF

Til populering og opdatering af et LDAP-katalog anvender man i dag fil-formatet LDIF. Fordelen er, at det er en velindarbejdet teknik. Ulempen er, at det kan kræve nedlukning af LDAP-kataloget at importere LDIF-filen, det kræver administrator-adgang og, at det i øvrigt involverer manuelle arbejdsgange.

6.1.2 DISP

Et alternativt til LDIF er X.500 DISP (Directory Information Shadowing Protocol). Denne protocol anvendes til replikering ved distribuerede og replikerede kataloger. Om man anvender LDIF eller DISP afhænger af konteksten samt hvilke protokoller/teknikker leverandøren af det pågældende katalog understøtter.

⁶ Provisionering dækker i denne sammenhæng over tildeling, opdatering og nedlæggelse af brugerkonti, ressourcer og retteligheder.

Det skal dog her bemærkes, at der fremadrettet peges på SPML, version 2.0 (behandles i afsnit 6.1.5) i en SAML konvolut til provisionering af brugerdata mod systemer. Dette understøtter udvikling af nye systemer baseret på web-services og med SOA arkitektur.’

6.1.3 LDAP directory synkronisering

Der kan også etableres synkronisering i mellem LDAP-kataloger – både til etablering af flere servere, der er synkroniserede, og til føddning af meta-directories. Disse løsninger er dog implementeringsspecifikke og kræver nok relativt tæt kobling i mellem de involverede kataloger.

6.1.4 DSML

Synkronisering via mere løs kobling er mulig ved hjælp af Directory Services Markup Language standarden. DSML 2.0 specificerer hvorledes directory information og ændringer kan beskrives i XML. Bruger-katalog-information kan således udveksles mellem forskellige leverandørers directory-produkter via de samme kanaler som anden webservices trafik. Standarden har ingen specifikation af, hvorledes informationen kan overføres fortroligt, så ved følsom information må det forudsættes, at der på anden vis er etableret en sikker forbindelse. Leverandører som IBM, Novell, Microsoft, Sun og Oracle såvel som opensource-produktet OpenLDAP har støtte for DSML i deres directory-produkter.

6.1.5 SPML

DSML, som blev beskrevet i forrige afsnit retter sig mod håndtering af information i bruger-kataloger. Imidlertid er korrekt bruger-katalog-information blot en del af hele provisionerings-processen, hvor en bruger tildeles de nødvendige ressourcer og rettigheder for at kunne udføre sin opgave. For organisationer, som anvender en automatiseret provisioneringsproces vil standarden Service Provisioning Markup Language (SPML) være relevant. SPML 1.0 inkluderer dele af DSML 2.0, og har to formål:

- Automatisering af it-mæssige provisioneringsopgaver. Via en standardiseret måde at foretage provisionering inklusiv en nem måde at indkapsle sikkerheds og kontrol-behovene i provisioneringssystemerne understøtter SPML automatisering af provisioneringsopgaverne.
- Interoperabilitet i mellem forskellige provisioneringssystemer. Via SPML-grænseflader kan provisioneringssystemer fra forskellige leverandører indgå i fælles proces.

Med SPML fås en standardiseret måde at sende følgende provisionerings-hændelser på:

- Tilføj/Opret
- Slet
- Opdater
- Forespørg

I forhold til håndtering af eksterne brugere er det den interoperabilitet, som SPML tilbyder, der er interessant. Spørgsmålet er, om SPML 1.0 er rig nok til de behov, der er for provisionering af brugere på kryds og tværs indenfor det offentlige. Det kræver en række detaljerede use cases, før det kan afgøres⁷

6.2 Unik repræsentation af ressourcer

Ressourcer, der skal beskyttes, kan beskrives unikt ved hjælp af Extensible Resource Identifiers (XRI), der er en videreudvikling af URL/URI-notationer. Blandt målene med XRI er definition af et URI schema og tilhørende URN namespace, som muliggør en transport- og applikationsuafhængig identifikationsmetode,

⁷ Der er en version 2.0 af SPML under udvikling, som understøtter flere behov. Til dette arbejdet har IBM overdraget WS-Provisioning-specifikationen til OASIS som input til dette arbejde. Det er muligt at standarden i forbindelse med dette arbejde skifter navn til fx WS-Provisioning.

der understøtter distribuerede services for brugerkataloger, og muliggør identifikation af ressourcer (herunder personer og organisationer).

XRI anvendes blandt andet i forbindelse med eXtensible Access Control Markup Language (XACML), der giver en standardiseret måde at beskrive politikker for rettighedsstyring og udseende af adgangsanmodninger.

Der er et initiativ i gang mellem *Distributed Management Task Force (DMTF)*, *Network Applications Consortium (NAC)*, og *Open Group* vedrørende definition af et rammeværk for "Common Core Identity Representations". Videnskabsministeriet deltager blandt andet i dette arbejde for at undersøge, om et sådant rammeværk vil resultere i nogen konflikt i forhold til anvendelse af XRI til repræsentation af ressourcer.

Umiddelbart antages det, at der i første omgang kan anvendes en URI-notation for identifikation af ressourcer, som siden hen uden store ændringer vil kunne indgå i et samlet koncept baseret på XRI.

6.3 Synkronisering af ressource-beskyttelse-information

Ressourcebeskyttelsesinformation kan formuleres som politikker i eXtensible Access Control Markup Language (XACML).

XACML giver en struktur for beskrivelse af politikker for tilgang til ressourcer, samt en metode til at forespørge om adgang til ressourcer.

XACML-politikker kan udveksles imellem organisationer ved hjælp af SPML. Adgangsanmodninger i XACML kan oplagt overføres ved hjælp af SAML.

Det er verificeret af Veterans Administration i USA at opbevaring af XACML politikker i LDAP kataloger er praktisk muligt⁸. Det bør således også være muligt at udveksle XACML politikker via DSML.

7 Videre arbejde

Det videre arbejde i forhold til ovenstående overvejelser inkluderer validering af, at de nævnte standarder er de bedste valg mht. anvendelse i fællesløsninger, som måtte blive etableret i den kommende tid – såvel som med henblik på inkludering af standarderne som anbefalinger i OIO Referencemodel for tværgående brugerstyring.

⁸ www.va.gov/rbac/docs/Veterans_Administration_Lab_Eval_of_XML_Technologies.pdf

8 Appendiks A - Definitioner

Dette appendiks indeholder definitioner på engelsk af begreberne *interoperabilitet* (Interoperability), *samarbejde* (Collaboration), og *nytænkning af måden offentlige ydelser leveres på* (Transformation). Definitionerne er hentet fra en Canadisk e-Government præsentation⁹.

Interoperability

- “The ability of different types of computers, networks, operating systems, and applications to work together effectively in order to exchange information in a useful and meaningful manner.” *SATBs Aug 10, 2004*
- The end result is seamless sharing of trusted and reliable information between partners in compliance with Government of Canada policies, security and privacy directives.

Collaboration

- “A process through which parties who see different aspects of a problem can explore constructively their differences and search for (and implement) solutions that go beyond their own limited vision of what is possible.” *Taylor-Powell et al., 1998*

Business Transformation

- Fundamentally rethinking and redesigning the underlying structure of a government program service and how it is delivered. (TBS - BTEP).
- Business Transformation will result in the improvement of the quality and / or delivery of Programs, Services and Processes.
- Attempting to achieve dramatic improvements in:
 - Client satisfaction
 - Cost efficiencies / savings
 - Achievement of policy outcomes / compliance
 - Accountability and transparency

9 Appendiks B - Yderligere information

Dette fællesoffentlige arbejde i forbindelse med tværgående brugerstyring er beskrevet på

<http://www.oio.dk/arkitektur/brugerstyring>

⁹ *Leadership through Partnership: One step at a time* af Alistair Rondeau - PSEPC - Data Standards Secretariat Mgr.; Ed Buchinski - TBS/CIOB - IM E-enabler POC PM; Aziz Abouelfoutouh - PWGSC - Registry/Repository PM; Susan Berg - HC / RCMP - SSDUE II PM; Ken Dagg - Fujitsu Consulting - Industry Partner

Information om nogle af de aktiviteter inden for it-sikkerhed, som Videnskabsministeriet varetager findes på

<http://www.oio.dk/sikkerhed>

Information vedrørende arbejdet med at implementere en fælles standard for styring af it-sikkerhedsprocesser i staten findes på

<http://www.oio.dk/itsikkerhed/isis>