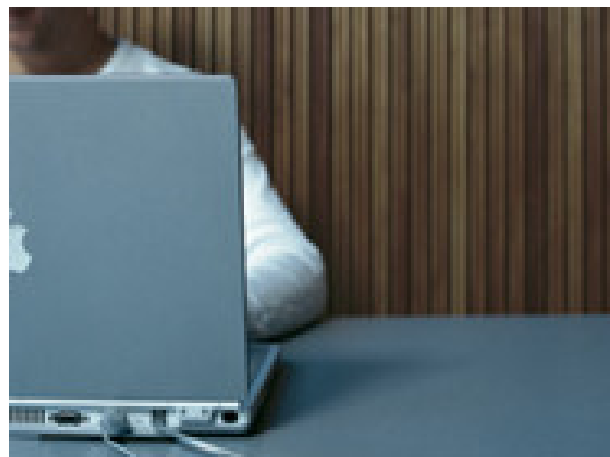

**Anbefalinger til kommuner
vedrørende brugerstyring i
forbindelse med
kommunalreformen**



Videnskabsministeriet i samarbejde med KL

November 2005

Anbefalinger til kommuner vedrørende
brugerstyring i forbindelse med
kommunalreformen

Udgivet af:

Ministeriet for Videnskab,
Teknologi og Udvikling
Bredgade 43
1260 København K

Telefon: 3392 9700
Fax: 3332 3501

Publikationen udleveres gratis,
så længe lager haves ved
henvendelse til:

IT- og Telestyrelsen. danmark.dk
Telefon: 1881
sp@itst.dk
www.netboghandel.dk

Publikationen kan også hentes
på Videnskabsministeriets
Hjemmeside: <http://www.vtu.dk>
ISBN (internet):

Tryk:

Oplag:
ISBN:

>

Anbefalinger til kommuner vedrørende brugerstyring i forbindelse med kommunalreformen

Videnskabsministeriet i samarbejde med KL
november 2005

Indhold

>

1	Introduktion	6
1.1	Formål	6
1.2	Baggrund	6
1.3	Vejledningens struktur	7
1.4	Læsevejledning	7
2	Hvad er brugerstyring	8
2.1	Generelt	8
2.1.1	Administration og styring	9
2.1.2	Udstedelse af akkreditiver	9
2.1.3	Lagring	10
2.1.4	Autenticitetssikring	10
2.1.5	Autorisation	10
2.1.6	Logning og kontrol	11
3	Brugerstyring i dag	12
3.1	Generelt	12
3.2	Oprettelse og nedlæggelse af brugere	12
3.3	Kommunale it-brugere	12
3.4	Brugerkataloger	13
3.5	Digital Signatur	13
3.6	Overblik og styring af rettigheder	13
3.7	KMD profiler	13
3.8	Logning	14
3.9	Mobile løsninger	14
4	Nye udviklingstendenser	15
4.1	Generelt	15
5	Fremtidig krav til brugerstyringsløsninger	17
5.1	Generelt	17
5.2	Simplificeret Sign-On	19
5.3	Nulstilling af kodeord	20
5.4	Brugeradministration og selvbetjening	20
5.5	Anvendelse af digital signatur	21
5.6	Sammenhæng mellem brugerkataloger - Directory-services	21
5.7	Provisionering og workflow	22
5.8	Politikker, revision med mere	22
5.9	Sikre services til tværgående samarbejde	23
5.10	Afrunding	23
6	Forslag til sammenlægningsaktiviteter	24
6.1	Generelt	24
6.2	Fastlæg pejlemærker for brugerstyring i den nye kommune	24
6.3	Fastlæg ambitionsniveau i forhold til sammenlægningsopgaven	24
6.4	Understøttelse af Digital Signatur	25
6.5	Fastlæg organisatorisk ansvar	26
6.6	Bestem hvilken information om brugere, der skal kunne anvendes i forskellige sammenhænge	29
6.7	Migrering af kataloger	29
6.8	Stikord til aktivitetsbeskrivelserne	30

7	Rammesystemer	32
	7.1 Introduktion	32
	7.2 Generelt	32
8	Fastlæggelse af ambitionsniveau og faser	35
	8.1 Introduktion	35
	8.2 Modenhedsfaser	35
	8.2.1 Overlev, Standardiser eller Integrer?	35
9	Anbefalinger vedrørende format på bruger-id	38
	9.1 Generelt	38
	9.2 Bruger ID	38
10	Anbefalinger vedrørende basis datamodel for bruger	41
	10.1 Definition af bruger	41
11	Katalog-struktur	44
	11.1 Indledning	44
	11.2 Generelle overvejelser	44
	11.3 Generelle anbefalinger	44
12	Anbefalinger vedrørende interoperabilitet med andre myndigheders løsninger	46
	12.1 Indledning	46
	12.2 Niveauer af autenticitetssikring	46
	12.3 Fælles arkitektur for tværgående autenticitetssikring	47
	12.4 RBAC – Rollebaseret adgangskontrol	47
	12.5 Andet	48
13	Checklister	49
14	Principper/Pejlemærker	51
	14.1 Forslag til principper/pejlemærker for brugerstyring	51
15	OCES – Digital Signatur	53
	15.1 Indledning	53
	15.2 Traditionel anvendelse af OCES certifikater	53
	15.3 Ldapter	53

1 Introduktion

1.1 Formål

Formålet med denne vejledning er at hjælpe den enkelte kommune med området brugerstyring inden for en it-sammenlægning. Dette sker via anbefalinger om hvilke valg, der skal foretages, og hvilke aktiviteter man skal i gennem.

Samtidig er målet, at anbefalingerne peger på løsninger, der kan spille sammen med andre myndigheders brugerstyringsløsninger. Dermed minimeres sikkerhedsmæssige, administrative og tekniske omkostninger ved udbredelse af løsninger til digital forvaltning, som går på tværs af myndigheder, private og virksomheder.

Kommunalreformen vil for hovedparten af de danske kommuner betyde, at forskellige it-miljøer og it-brugergrupper skal sammenlægges. Kommunerne tilføres en række væsentlige nye opgaver og en større gruppe nye medarbejdere fra amterne. Samtidig skal kommunerne fungere som én indgang til det offentlige, **og** vil på den baggrund også have medarbejdere, der skal have brugerrettigheder i en række andre myndigheders it-løsninger. Endelig må det også forventes, at mængden af it-løsninger og andelen af medarbejdere, der er it-brugere i den enkelte kommune, vil vokse i forbindelse med den generelle udbygning af digital forvaltning.

Helt konkret er målet for dette dokument at medvirke til at understøtte en digital forvaltning med en effektiv brugeradministrationen. Det skal være let at oprette en bruger, at tildele brugeren adgang og rettigheder på netværket og helt generelt have styr på brugeren, brugerens placering i organisationen og dennes ansættelsesmæssige forhold. Ligeledes skal de være nemt og sammenhængende for egne brugere og samarbejdspartnere at få adgang til de it-løsninger, som de har behov for.

Ovenstående resulterer i nye behov og krav til brugerstyring. Kommunalreformen betyder således, at de nye kommuner skal træffe beslutninger om brugerstyringsløsninger. Det er en oplagt mulighed at valgene, der foretages, i høj grad foretages ud fra fælles anbefalinger, således at der så vidt muligt anvendes samme standarder og samme begrebsmodeller.

BEMÆRK – Den nuværende udgave af vejledningen indeholder afsnit med områder, som kun er beskrevet i stikordsform. Det er planen senere at opdatere vejledningen på baggrund af konkrete erfaringer. Det er dog vurderingen at vejledningen i sin nuværende form er et brugbart og vigtigt værktøj for kommuner, som står overfor sammenlægning. Derfor publiceres vejledningen selvom visse områder ikke er detaljeret beskrevet.

1.2 Baggrund

Baggrunden for vejledningen er dialog med en række medarbejdere i danske kommuner, primært kommunerne Stenløse, Ølstykke og Ledøje-Smørum (som bliver til Egedal kommune), Søllerød og Birkerød (som bliver til Rudersdal kommune), Københavns kommune og Gentofte kommune men derudover også andre kommuner, repræsentanter, leverandører, myndigheder etc.

På alle relevante punkter tager vejledningen afsæt i det fællesoffentlige it-arkitekturarbejde og specielt i arbejdet vedrørende en fællesoffentlig referencemodel for tværgående brugerstyring inden for det offentlige.

1.3 Vejledningens struktur

I det følgende forklarer vi kort, hvad vi mener med brugerstyring. Vi opsummerer desuden en række karakteristika ved den nuværende håndtering af brugerstyring i en række kommuner. Nye udviklingstendenser for kommunerne vil stille krav til måden, brugerstyring håndteres på, og vi diskuterer nogle af disse.

På basis af dette gennemgår vi en række behov, som de nye kommuner bør beslutte, om deres brugerstyringsløsninger skal opfylde. Og hvis ja: Hvornår?

Vi giver forslag til en række aktiviteter, som kan indgå i den enkelte kommunes brugersammenlægningsprojekt, og vi kommer med forslag til valg af standarder, datamodeller etc.

Vi diskuterer i hvor høj grad, der findes rammesystemer til brugerstyring, som matcher kommunernes behov.

1.4 Læsevejledning

Dokumentet består af 15 kapitler, der umiddelbart kan læses uafhængigt. De grundlæggende udfordringer er søgt beskrevet i de første 6 kapitler, hvorefter mere specifikke emner behandles.

Kapitel 1 – indledningen giver et kort overblik over formålet med vejledningen. Kapitel 2 til 5 omhandler brugerstyring i kommunerne generelt, den nuværende situation og fremtiden.

Kapitel 6 giver forslag til sammenlægningsaktiviteter.

Kapitel 7 omhandler rammesystemer, som beskrives ganske kort. Dette leder læseren over i Kapitel 8, der er fastlæggelse af ambitionsniveauer og faser.

Kapitel 9 omhandler standarder for bruger-id'er.

Kapitel 10 og 11 omhandler indhold og struktur af kataloger.

Kapitel 12 omhandler interoperabilitet med andre myndigheders løsninger, mens at Kapitel 13 er første udgave til en checkliste til brugerstyring og hvad man skal gøre sig af overvejelser. Listen er ikke udtømmende.

Kapitel 14 giver forslag til Pejlemærker, og der slutes af med Kapitel 15 om digital signatur, hvor bl.a. muligheder for at knytte udstedelse og nedlæggelse af digital signatur tættere sammen med resten af brugeradministrationen beskrives ganske kort.

Med bare lidt kendskab til it vil de fleste af ovenstående kapitler kunne læses uden videre. Læsere uden interesse for teknik kan med fordel læse til og med kapitel 6. Specielt kapitel 10 og 11 er dog nok af lidt mere teknisk karakter. Formålet med dokumentet har været at give et overblik over de udfordringer kommunerne står over for i forbindelse med brugerstyring og kommunalreformen. Det er ikke tænkt som et teknisk dokument der behandler alle emner i detaljer.

2 Hvad er brugerstyring

2.1 Generelt

Brugerstyring handler om, hvordan brugere, services og ressourcer identificeres, hvilke rettigheder de skal have, hvordan der sikres sporbarhed i forhold til deres handlinger samt den nødvendige, bagvedliggende administration.

I ældre it-løsninger har brugerstyring normalt været en integreret del af løsningen. Det har betydet, at der for hver ny løsning ofte kom en ny måde at håndtere brugere på.. Resultatet blev ofte en øget administrativ byrde. Dette er desværre ofte stadig tilfældet, selvom der er tiltag til, at brugerstyring kan blive eksternaliseret¹ i nye it-løsninger, således at denne funktionalitet kan varetages af en fælles brugerstyringsløsning. Sammen med den fortsatte decentrale brugerstyring i nye systemer betyder væksten i antallet af brugere, at brugeradministration løbende bliver mere og mere kompleks og tidskrævende. Et problem man, bl.a. inden for sundhedssektoren, har været opmærksom på i mange år.

Brugerstyring er et meget vigtigt element i det samlede it-sikkerhedsarbejde, men udgør dog kun en delmængde. For eksempel indgår ”perimeter-forsvar” med firewalls, anti-virus etc. også i it-sikkerhedsarbejdet uden at disse aktiviteter har noget væsentligt at gøre med brugerstyring.

Omvendt skal brugerstyring også varetage interesser ud over it-sikkerhed.

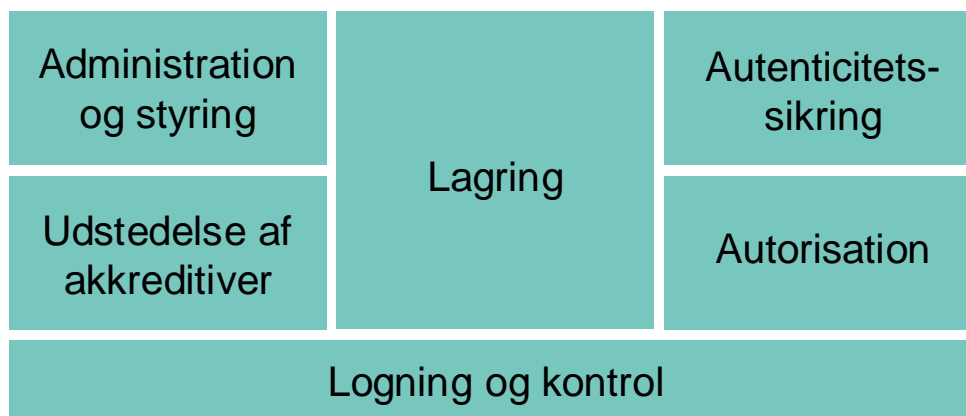
Her er kort opsummeret nogle af de områder, som brugerstyring spiller en væsentlig rolle inden for:

- It-sikkerhed
- Risikominimering
- Lovmæssige krav (overholdelse af persondataloven osv.)
- Bedre service til borgere og virksomheder
- Effektivisering
 - Hensigtsmæssig administration
 - Brugervenlighed
- Flexibilitet og interoperabilitet
 - Via standardisering og integration

Disse områder påvirker de krav, man skal stille til en brugerstyringsløsning. Mens de lovmæssige krav i princippet ikke er til diskussion, vil man for de øvrige områder skulle overveje hvilke fordele, man kan høste i forhold til de krav, man stiller. Flere krav vil ofte betyde en øget kompleksitet.

Til illustration af, hvad vi taler om, når vi siger brugerstyring, vil vi anvende modellen i figur 2.1:

¹ Med eksternaliseret forstås at brugerstyringen kan betragtes som et modul, der kan adskilles fra selve it-løsningen og så administreres fra et andet system. Brugeroplysningerne skal stadig bruges, men administreres således ikke i selve systemet.



Figur 2.1. Overordnet referencemodel for brugerstyring²

De forskellige områder på figur 1 dækker over væsentlige processer, services og teknologier i forbindelse med brugerstyring. Områderne vil kort blive gennemgået i det følgende, så der kan komme lidt flere ord på, hvad de enkelte kasser dækker over.

Dele af den efterfølgende beskrivelse er kan virke teoretisk. Man kan springe resten af kapitel 2 over i første omgang, og så gå tilbage senere, hvis der er nogle af kasserne i figuren, som man gerne vil have beskrevet i detaljer.

2.1.1 Administration og styring

Administration og styring omfatter processer og services til håndtering af livscyklus for it-brugere og it-ressourcer. Services omfatter bl.a.:

- Provisionering (bl.a. tildeling, opdatering og nedlæggelse af brugerkonti³, ressourcer og rettigheder)
- Workflow – automatisering af provisionering, processer etc.
- Delegering af administrative rettigheder inkl. selvbetjening
- Historik

Bemærk, at administration og styring også kan omfatte egne brugeres konti i eksterne systemer i forbindelse med tværgående brugerstyringsløsninger.

2.1.2 Udstedelse af akkreditiver

Et akkreditiv eller sæt af akkreditiver er noget, som man kan præsentere for at bevise sin identitet, eller for at bevise at man har fået tildelt nogle rettigheder.

² Modellen er udarbejdet på baggrund af en række overordnede scenarier for tværgående brugerstyring med inspiration i en tilsvarende model fra Booz Allen Hamilton.

³ Brugerkonti omfatter netværk/print, applikationsspecifikke konti (fx e-mail), portalkonti mm.

Eksempler på akkreditiver er digital signatur, bruger-id/kodeord, tokens, skabelon med biometriske data (fx fingeraftryk), smart cards, mm. Udstedelse af akkreditiver omfatter, foruden udstedelse, også vedligehold og nedlæggelse samt afstemning/sammenknytning af individuelle akkreditiver. Til udstedelse af akkreditiver tilknyttedes services, der omfatter kontrol af beviser på brugers identitet samt registrering og udstedelse af akkreditiver.

2.1.3 Lagring

Lagring vedrører samling og beskyttelse af de informationer, som udgør en brugers digitale identitet. Hver enkelt information om en bruger kalder vi en attribut. Standard pakke-it-løsninger gemmer ofte bruger-attributter i LDAP kataloger.

Services i forbindelse hermed er lagring og fremfindelse⁴/attributservice. Tekniske koncepter og løsninger til lagring omfatter bl.a. virtualisering, metadirectory⁵ services og enterprise directories. Synkronisering af brugere (digitale identiteter/sæt af attributter) på tværs af organisatoriske skel falder også inden for rammerne af lagring.

2.1.4 Autenticitetssikring

Autenticitetssikring har til formål at verificere og/eller validere en brugers/services autenticitet baseret på et sæt af attributter fra brugerens/servicens digitale identitet.

Services, som anvendes til autenticitetssikring, omfatter politik-håndhævelsesnoder⁶, politik-beslutningsnoder⁷ og akkreditiv-validering.

2.1.5 Autorisation

Autorisation drejer sig om validering og/eller verifikation af en brugers/services rettigheder til en specifik service. Verifikationen baseres på et sæt af attributter fra brugerens/servicens digitale identitet. Services inkluderer lagring af politikker.

Tekniske løsninger til autorisation inkluderer rollebaseret adgangskontrol, regelbaseret adgangskontrol, attributbaseret adgangskontrol og formålsbestemt adgangskontrol.

⁴ Fremfindelse er i denne sammenhæng lig med det engelske ord discovery.

⁵ Directory = Katalog. Begge betegnelser benyttes i dette dokument.

⁶ Politik-håndhævelses-node dækker over den engelske betegnelse Policy Enforcement Point.

⁷ Politik-beslutnings-node dækker over den engelske betegnelse Policy Decision Point.

2.1.6 Logning og kontrol

Logning drejer sig om registrering og beskyttelse af information om brugerens/servicens aktiviteter, således at der i relevante tilfælde er mulighed for at etablere et revisionsspor eller udføre andre kontroller i forhold til anvendelsen af it-systemer

Services inkluderer i denne forbindelse logning, proaktiv monitorering, udtræk af kontrolrapporter.

Alle elementerne i denne referencemodel er relevante for brugerstyring i den enkelte organisation såvel som ved tværgående brugerstyring.

3 Brugerstyring i dag

3.1 Generelt

I dette kapitel skitserer vi en række fælles punkter for, hvorledes brugerstyringsopgaven løses i dag. Udgangspunktet er møder med en række af de kommuner, der bliver til hhv. Egedal og Rudersdal samt Gentofte og Københavns kommune.

Vi diskuterer ikke fordele og ulemper ved den nuværende situation. Vi beskriver punkterne således, at de kan indgå i de følgende kapitels overvejelser om, hvorledes en ny brugerstyring kan/skal tilrettelægges.

3.2 Oprettelse og nedlæggelse af brugere

Generelt oprettes it-brugere i kommunerne inden for en eller flere af følgende tre grupper af systemer:

- KMD-løsninger, som afvikles på mainframe og tilgås via 3270-skærbilleder
- Fælles lokale it-løsninger, som netværksdrev, e-mail, kalender, ESDH etc.
- It-løsninger vedrørende et fagområde, fx omsorgsløsning, arbejdsmarkedsportal etc.

Institutioner, som for eksempel børnehaver og plejehjem, serviceres ofte af rådhusets it-afdeling. Billedet er mere blandet for skolerne og i nogen grad også bibliotekerne. I nogle kommuner håndterer skolerne selv alt vedrørende it, mens rådhusets it-afdeling andre steder står for drift af netværk og administrative løsninger.

Generelt gælder der følgende vedrørende brugeroprettelse og brugernedlæggelse i kommunerne:

- Oprettelse af nye brugere sker via manuelle procedurer (primært gentageligt tastearbejde)
- Nedlæggelse af eksisterende brugere, f.eks. i forbindelse med fratrædelser, sker ligeledes via manuelle procedurer.
 - It-afdelingen må periodisk checke lister over ansatte i forhold til registrerede brugere
 - Kontrol af valide brugere sker sjældent i systemer, der administreres af fagområder som fx omsorgssystemer.

3.3 Kommunale it-brugere

Før

- Kommunens it-brugere har traditionelt været blandt de administrative medarbejdere. Denne gruppe er kendetegnet ved, at den personalemæssige udskiftning er relativt lille.
- Antallet af it-brugere blandt det udførende personale (fx social- og sundhedsassistenter, vejfolk etc.) er relativt begrænset.

Nu

- Flere og flere medarbejdere er (eller bliver) it-brugere, fremskyndet af teknologier som PDA'ere og bærbare computere.
- Medarbejderudskiftningen er stigende blandt it-brugere, så behovet for oplæring er stiger.

3.4 Brugerkataloger

- Hver bruger oprettes i flere uafhængige brugerkataloger (KMD, netværks-directory, e-mail-directory, ESDH, individuelle fagsystemer, evt. intranet etc.).
- Nogle brugerkataloger synkroniseres indholdsmæssigt og/eller med kodeord, men dette gælder langt fra alle.
- Trods mange forskellige systemer anvendes relativt få bruger-id'er. Typisk er der ingen synkronisering mellem de enkelte systemer.

3.5 Digital Signatur

- Digital signatur til medarbejdere er hidtil kun uddelt ad-hoc, fx til forbindelse til statslige systemer inden for beskæftigelsesområdet.

3.6 Overblik og styring af rettigheder

- Det er svært at få et samlet overblik over, hvilke ressourcer og rettigheder en bruger har.
 - KMD bruger-id anvendes i nogle kommuner til at angive organisatorisk tilhørsforhold.
 - Rettighedstildeling sker ofte på basis af anden brugers rettigheder. Den anvendes som en slags profil og er ikke baseret på den nye brugers konkrete jobfunktion.
- Politikker for adgang og anvendelse af it-udstyr, løsninger og informationer administreres i de enkelte systemer ofte uden standarder for hvordan regler/politikker angives.
- Organisatorisk tilknytning anvendes i høj grad til rettighedsstyring, men der er ingen central vedligeholdelse af organisationsstrukturen i relation til it-systemer. Som eksempler, hvor organisatorisk tilknytning anvendes, kan nævnes:
 - KMD-systemer via KMD-LOS
 - Netværk, diske, e-mail via organisationstruktur i katalog
 - ESDH vedligeholder egen organisationsstruktur

Alle disse steder vedligeholder man sin egen udgave af kommunens organisation.

3.7 KMD profiler

- KMD-profiler kan være uoverskuelige på grund af mængden og mangel på navngivningsstandarder
 - Behov for skabelon-profiler, med rettighedsdefinitioner, som svarer til generelle funktionsmæssige roller
 - Behov for navngivningsregler

3.8 Logning

- Logning udføres i de enkelte systemer i forhold til lovmæssige forskrifter.
- Ingen standardisering af log-filer mht. indhold og formater.
- Logfilerne er der, men bruges generelt ikke (gælder ikke log i forbindelse med internettrafik).

3.9 Mobile løsninger

- PDA'er og lignende mobile løsninger anvendes i stigende omfang til e-mail/kalender, f.eks. Københavns Kommune gør kraftig brug af denne teknologi.
- Kobling til fx omsorgssystem udnyttes mere og mere. Flere kommuner er langt fremme i denne udvikling, mens andre kommuner kører mere 'traditionelt'.

I næste kapitel vil vi i stikordsform gennemgå en række udviklingstendenser, som vil stille nye krav til den måde, kommunerne håndterer brugerstyring på fremover.

4 Nye udviklingstendenser

4.1 Generelt

I forbindelse med den generelle udvikling inden for digital forvaltning, og i særdeleshed i forbindelse med kommunalreformen, opstår der en række nye forhold, som får betydning for de fremtidige krav til brugerstyring. Vi skitserer nogle af dem i dette kapitel, således at de også kan indgå i overvejelserne i de følgende kapitler om, hvorledes den nye brugerstyring skal tilrettelægges.

- Kommunerne vil bestå af større organisationer med større grad af geografisk spredning. Det vil bl.a. få følgende konsekvenser:
 - Flere administrative centre, mere hjemmearbejde, flere medarbejdere som kommer ud til borgerne.
 - Chefer har ikke nødvendigvis alle medarbejdere i deres afdeling på samme fysiske adresse.
 - Systemejer-rollen vil muligvis ændre sig. Systemejeren er måske fremover i mindre grad "almindelig" bruger af systemet.
- Der vil komme en større administrativ byrde i forbindelse med administration af egne brugeres rettigheder i eksterne løsninger
 - Fx ToldSkat, Beskæftigelsesområdet, Miljø etc.
- En større andel af de ansatte bliver it-brugere, og nye klienttyper skal understøttes. Eksempelvis:
 - PDA/Smartphone til omsorgs-ansatte
 - E-mail til alle
 - Flere eksterne brugere (hjemmearbejde, mobile arbejdere)
- Større administrativ byrde mht. vedligeholdelse af it-brugere som følge af større personalemæssig udskiftning. Der kommer flere it-brugere blandt det udførende personale, og her er udskiftningen større end hos det administrative personale.
- Nye måder at arbejde sammen på:
 - Flere opgaver løses i projekter, hvor deltagerne kommer fra forskellige fagområder.
 - Mere samarbejde med andre myndigheder i forbindelse med, at kommunen bliver "én indgang til det offentlige": Skat, Beskæftigelse, Pas/Kørekort, Servicefællesskaber, fra arbejds-kommune til bopæls-kommune etc.
- Behov for at it-systemerne er oppe ud over almindelig arbejdstid. Dette skaber øget behov for automatiserede overvågningsløsninger samt beredskab, der kan reagere på fejl/nedbrud uden for "almindelig åbningstid".
- Øget anvendelse af elektronisk identifikation (digitale akkreditiver).
Eksempler:
 - Intern brug af signaturer i forbindelse med blanketter
 - Officiel kommunikation med borgere, andre myndigheder og leverandører
 - Intranet/Intern portal (Bruger/Rolle-profil)

- Behov for generel bevidstgørelse om organisationens sikkerhedspolitikker og lovmæssige krav
 - Øget krav til god databehandlingsskik, sporbarhed og autorisation i forhold til opgaven
- Behov for at kunne indlejre sikkerhedspolitikker direkte i de tekniske løsninger modsat manuel håndtering af den enkelte bruger.
- Behov for større grad af dokumentation i forbindelse med oprettelse af it-brugere. Afstanden fra brugerstyringsadministrationen til den enkelte bruger bliver større pga. større organisationer. Man 'kender' ikke sine brugeres præcise jobfunktioner.
 - Oprettelse af SLA'er/Resultatkontrakter
 - På vej til "ITIL⁸ for brugerstyring"
 - Krav til potentiel out-sourcing af it-driften

Nogle af tendenserne slår igennem allerede i forbindelse med gennemførelse af kommunalreformen. Andre repræsenterer trends, som vil vinde indpas i en "glidende" overgang i de kommende år.

Selvom tendenserne kun er præsenteret i stikordsform, er det tydeligt, at de nye kommuner er nødt til at gøre sig overvejelser om organisering, proces og tekniske løsninger til brugerstyring. Løsningerne på disse områder skal have en bredere rækkevidde, end de har i dag. Vi vil i næste kapitel tage hul på, hvilke krav de nye behov stiller til tekniske løsninger og standarder.

⁸ The IT Infrastructure Library

5 Fremtidig krav til brugerstyringsløsninger

5.1 Generelt

I forhold til de nuværende udfordringer og fremtidige tendenser for brugerstyring i kommunerne har vi opstillet en liste over relevante funktionaliteter. Listen tager udgangspunkt i en kommune, som forventes at skulle implementere en samlet brugerstyringsløsning på kort eller lang sigt, hvis det ikke allerede er sket:

- SSO, Simplificeret Sign-On.
- Nulstilling af kodeord.
- Mere effektiv brugeradministration og selvbetjening, herunder også administration af egne brugeres rettigheder i eksterne løsninger.
 - Standardiseret logning og kontrol
 - Sporbarhed i forbindelse med revision
 - Historik på brugeradministrationen
 - Standardisering af bruger-id'er
- Anvendelse af digital signatur (OCES) til kryptering, signering og uafviselighed for alle it-brugere.
- Sammenhæng mellem brugerkataloger og ”telefonbogsservice”, som ud over kontaktinfo også dækker kompetencer, interesser, og organisatorisk ophæng (Directory-services).
- Samlet provisionering ved brugeroprettelse og workflow.
- Styring af politikker.
- Sikre services til tværgående samarbejde (udveksling af data, tilgang til services etc.).

I tabel 1 nedenfor illustreres det, hvilke af de ovenfor nævnte funktionaliteter, der er relevante i forbindelse med de nuværende og fremtidige tendenser/behov inden for brugerstyring. Vi har gennemgået disse i kapitel 3 og 4.

Nuværende og fremtidige tendenser og behov	Tilsvarende funktionelle behov							
	SSO	Kode-ord	Adm.	Dig Sig	Dir-svs.	Prov. Wkflw	Politikker Revision	Sikkert samarb
Brugere er oprettede separat i forskellige applikationer, platforme mm.	X	X	X					
Manuelle arbejdsgange ved tildeling/ændring af brugeres rettigheder		X	X			X		
Administratorer får ikke altid besked om ansættelsesophør			X		X	X	X	
Funktion til administration af identitet og rettigheder i flere forskelligesystemer	X		X	X	X	X		
Forskellig information om brugere i forskellige systemer					X	X		
DigitalSignatur uddelt ad hoc				X	X	X		X
Svært at få samlet overblik over brugers ressourcer og rettigheder			X		X		X	
Politikker for autorisation administreres i forskellige systemer					X		X	
Ingen samlet vedligeholdelse af organisationsstruktur					X	X	X	
Meget begrænset,og forskelligartet,logning ud over lovkrav							X	
Større geografisk spredning, flere administrative centre			X			X		X
Flere rettigheder i eksterne systemer skal adminstreres			X			X	X	X
Anvendelse af nye typer (mobile mm.) af klienter	X		X		X	X	X	
Nye tværgående samarbejds måder							X	X
Større personalemæssig udskiftning			X		X	X	X	
Større anvendelse af digitale akkreditiver				X				X
Bedre kommunikation og bevidstgørelse af politikker vedrørende sikkerhed mm.					X		X	
Behov for indlejring af sikkerhedspolitikker direkte i it-løsninger					X		X	X
Behov for større grad af dokumentation							X	

Tabel 1. Brugerstyringsfunktionalitet til understøttelse af tendenser og behov

Ovenstående er afledt af forretningsmæssige behov. Systembehov er ligeledes en faktor, og der vil være en del overlap med ovenstående. Backup mm. behandles ikke direkte i denne vejledning..

Der kan altså reelt i forhold til kommunerne argumenteres for indførelse af alle de nævnte brugerstyringsfunktionaliteter. Det betyder dog ikke, at det er nødvendigt at indføre dem alle på én gang (se kapitel 8 omkring ambitionsniveau).

Brugerstyringsfunktionaliteter diskuteres yderligere i slutningen af dette kapitel. Først beskrives de enkelte funktionaliteter lidt mere detaljeret.

5.2 Simplificeret Sign-On

Generelt er det indtrykket, at kommunale it-brugere i dag blot behøver to bruger-id'er: Et til KMD 3270-systemer og ét til netværk etc., for at få adgang til de it-systemer, der bruges i det daglige arbejde.

For de mest anvendte it-systemer sker der i mange tilfælde synkronisering af kodeord imellem systemerne.

Eksempel

Et eksempel på dette er den eksisterende arkitektur i Ledøje/Smørum. Brugere oprettes i Novel 6.5 (NDS) og replikeres over i AD ved brug af exchange 2003 server. Herefter synkroniseres bl.a. kommunens ESDH-system med AD, således at login og password kan anvendes direkte i ESDH-systemet.

For en række systemer vedligeholdes kodeord separat. Det er op til den enkelte bruger at huske kodeord og/eller sørge for manuelt at opdatere kodeordet i disse systemer, samtidig med at kodeordet til netværket opdateres.

Eksempel

Et typisk eksempel på dette er omsorgssystemer, der traditionelt har haft eget administrationsmodul til administration af brugere. Dette er gældende i både Stenløse og Søllerød kommune.

I takt med at flere medarbejdere skal benytte it-løsninger hos andre leverandører end KMD og/eller andre myndigheders systemer, vil brugeren få mere arbejde med at logge på forskellige systemer. Det bliver mere og mere udbredt, at der logges på med digital signatur, men realistisk set vil der stadig være systemer, hvor der logges på via bruger-id og kodeord. Det kan medføre flere kodeord, som skal huskes. Dette er i sig selv en udfordring for sikkerheden, idet man som bruger fristes til at skrive sine kodeord op for ikke at glemme dem.

Indførelse af løsninger, som reducerer antallet af gange, en bruger skal logge på systemer, Simplificeret Sign-On - forkortet SSO, medfører en direkte lettelse for brugeren i det daglige arbejde. Samtidig bliver den brugte tid og udgiften med at nulstille kodeord, som brugerne har glemt, sædvanligvis mindre (se evt. næste afsnit). Det medfører bl.a., at antallet af brugere per brugeradministrator hæves.

Løsninger med SSO inkluderer både *webbaseret single sign-on* til en række it-løsninger, som benyttes via en webbrugerflade, og *Enterprise SSO*. Enterprise SSO dækker også webbaserede løsninger samt fx ”tykke klienter”, mobile klienter, mainframe-løsninger etc. Denne type SSO-løsninger retter sig traditionelt mod den enkelte organisation, mens webbaseret single sign-on ved anvendelse af fællesoffentligt anbefalede standarder, typisk også anvendes til it-systemer på tværs af organisatoriske skel.

Det er værd at bemærke, at der med SSO ikke sigtes på, at brugeren kun skal logge på én gang og så har adgang til alle systemer. Dels kan der være tekniske udfordringer med hensyn til integration til ældre eller specielle systemer, dels kan der være kritiske systemer og systemer med følsomme data, som fordrer et højere sikkerhedsniveau end det generelle sign-on giver. I det sidste tilfælde findes der dog også SSO-løsninger,

som kan foretage en såkaldt ”step-up” autenticitetssikring, således at man fx kan logge sig på netværket enten med bruger-id/kodeord eller med digital signatur. Hvis man har logget sig ind med digital signatur, har man adgang til alle systemer, som SSO dækker. Hvis man har logget sig ind med bruger-id/kodeord og vil anvende et system, som kræver login med digital signatur, vil SSO-systemet registrere dette og bede brugeren om at logge sig på ved hjælp af digital signatur.

5.3 Nulstilling af kodeord

Nulstilling af glemte kodeord, specielt efter ferier og helligdage, lægger en stor arbejdsbyrde på helpdesk og administratorer. Løsninger, som tillader brugeren at nulstille sit kodeord via selvbetjening, vil reducere arbejdsbyrden for helpdesk og administratorer. Samtidig kan brugerne ofte få nulstillet deres kodeord hurtigere ved hjælp af selvbetjening fremfor at skulle kontakte helpdesk. De mest anvendte løsninger er webbaserede. Her indtaster brugeren blot sin email-adresse og svarer eventuelt på et ”challenge”-spørgsmål, hvorefter et nyt midlertidigt kodeord fremsendes via email. Der findes også telefon-løsninger, som er baserede på stemmegenkendelse, hvor en syntetisk stemme læser et midlertidigt kodeord op for brugeren. Udfordringen med mange kodeord, kan også imødekommes med anvendelse af en løsning, der synkroniserer kodeord imellem systemer. Sådanne løsninger bør dog kun anvendes til generelle systemer som netværk/print, email og intranet. Mere kritiske systemer og systemer med følsomme data bør, afhængigt af andre sikkerhedsforanstaltninger, sørge for, at brugeren anvender yderligere autenticitetssikring som token, digital signatur, smart card og lignende i kombination med kodeord.

5.4 Brugeradministration og selvbetjening

Bedre løsninger til administration af brugere og deres rettigheder inkluderer:

- Selvbetjeningsløsning, således at brugere kan opdatere en del af deres brugerinformation (bruger-katalogsattributter) på intranet og lignende. Der er her tale om stamdata dvs. adresseoplysninger, telefon etc.
- Støtte til rollebaseret adgangskontrol, hvor privilegier tilknyttes roller, og roller tildeles brugere.
- Delegeret rettighedsadministration, som i et fælles system tillader systemejere at administrere adgangsrettigheder til deres systemer, herunder:
 - Føderation af rettigheder med eksterne systemer, således at kommunens brugeres rettigheder til disse kan administreres lokalt i kommunens system (i stedet for at skulle foregå i de forskellige eksterne systemer).
- Samlet overblik over alle ressourcer og rettigheder, som er tilknyttet en given bruger.

Eksempel:

Gentofte kommune har en løsning, hvor der ligger en database parallelt med deres katalog. Databasen indeholder yderligere oplysninger ift. hvad der er gemt i kataloget. De 2 systemer er synkroniseret mht. fællesattributter.

Brugerne har fået udviklet et administrationsmodul, således at de selv vedligeholder data som adresse, telefonnummer mm. Endvidere kan afdelingsledere vedligeholde data for deres ansatte. Pga. synkroniseringen bliver kataloget automatisk opdateret med disse ændringer real-time. Rettigheder i forhold til. ESDH systemet vedligeholdes ligeledes her. På sigt skal databasen, og dermed også kataloget, fødes med data direkte fra HR/lønssystemet.

Administrative løsninger med føderation af rettigheder til eksterne systemer skal ses som et langsigtet behov, hvor alle nødvendige standarder ikke er fastlagt endnu. Der er dog en række standarder til understøttelse af føderation, som kommunerne kan begynde at efterspørge hos deres it-leverandører.

5.5 Anvendelse af digital signatur

Anvendelse af digital signatur eller mere korrekt 'digitale certifikater' til kryptering, signering og uafviselighed understøttes allerede delvist hos kommunerne. Med e-Dag2 er det blevet muligt for borgere/virksomheder at kommunikere sikkert med kommunerne og andre offentlige myndigheder via email.

Denne kommunikation foregår til og fra organisatoriske postkasser hos myndighederne. Yderligere tiltag inkluderer muligheden for, at offentligt ansatte kan kommunikere sikkert direkte med borgere og virksomheder via (krypteret) email. Samtidig kan tiltagene sikre, at andre ansatte i kommunen med rette autorisation, også vil have mulighed for at afkryptere emails, som en given medarbejder har modtaget. Krav om anvendelse af digital signatur i forbindelse med adgang til eksterne systemer og intern anvendelse, fx til underskrift på interne blanketter, fremmer også behovet for, at medarbejdere i kommunen skal have deres egen digitale signatur. Dette kræver bl.a., at udstedelse af digital signatur integreres med resten af provisioneringsprocessen og udstedelsen af andre digitale akkreditiver (som fx bruger-id/kodeord) samt deaktivering ved fratrædelse mm. Det kræver eventuelt også nye tekniske løsninger eller udvidelser af eksisterende løsninger. Det kan fx være til lagring af systembevis for en digital underskrift, lagring af samtykke afgivet med digital signatur eller udstedelse af tokens med digital signatur, som også giver mulighed for at logge på netværket etc.

Derudover skal der også etableres en håndterbar metode til administration af certifikater. Det kan ske ved etablering af sikre punkt-til-punkt-forbindelser mellem systemer i kommunen og systemer hos eksterne partnere.

5.6 Sammenhæng mellem brugerkataloger - Directory-services

Sikring af sammenhæng mellem forskellige brugerkataloger i kommunen er en vigtig forudsætning for mange af de funktionelle behov, der diskuteres i de foregående afsnit. Denne service kan etableres på forskellige måder:

- Et meta-katalog, som samler al information fra de andre brugerkataloger.
- Et hovedkatalog, som synkroniserer basisdata om brugere etc. med andre brugerkataloger.

- Et virtuelt directory, som bevarer data i de enkelte brugerkataloger, men som giver én samlet adgang til disse data.

Lige gyldigt hvilken tilgang der vælges, skal den sammenhængende brugerkatalogservice lagre samlet identitetsinformation (brugerprofiler) for personer, grupper af personer, organisationer, roller, udstyr og applikationer. De fællesoffentlige anbefalinger er, at services skal understøtte LDAP 3.0 protokollen. På sigt anbefales det også at efterspørge brugerstyringssystemer, som understøtter standarden til udveksling: Service Provisioning Markup Language (SPML). Kvaliteten af data i brugerkatalogsservicen sikres dels ved integration med forskellige anvendte brugerkataloger og dels ved integration med fagsystemer med relevant information som fx personale/lønssystem.

5.7 Provisionering og workflow

Der er effektiviserings- og sikkerhedsmæssige fordele ved at automatisere hele provisioneringsprocessen med oprettelse og nedlæggelse af brugerkonti, tildeling og ændring af adgangsrettigheder. Dette kan løses på forskellige måder. Én måde er, at ansættende afdeling udfylder en digital blanket, som chefen med ledelsesansvar og evt. andre, fx applikationsejere, godkender i et workflow. Herefter oprettes brugeren automatisk og tildeles de ressourcer og rettigheder, vedkommende har behov for. En workflow-understøttet digital blanket kan også anvendes til at give rettigheder til eksterne brugere, som fx konsulenter, medarbejdere fra andre kommuner etc. En mere integreret variant er, at det er personale/lønssystemet, som automatisk initierer godkendelses-workflowet. Det forudsætter dog, at det administrative arbejde med registrering af brugeren i personale/løn-systemet er på plads inden vedkommendes første arbejdsdag.

5.8 Politikker, revision med mere

Som nævnt i persondataloven vedrørende korrekt opførsel og korrekt brug af kommunens ressourcer og it-systemer kan kommunens politikker og lovkrav håndhæves og kommunikeres mere effektivt med it-understøttelse. Dette inkluderer også revision af, at gældende politikker og lovkrav overholdes.

Relevante politikker inkluderer klassificering og beskyttelse af data/information, regler for kodeord, politikker for autenticitetssikring/adgangskontrol/autorisation og politikker vedrørende privacy for det enkelte individ.

Der kan etableres en såkaldt policy-server, som indeholder politikker og understøtter håndhævelse af samlede sæt af politikker i flere it-systemer. Nogle politikker kan fastlægges af topledelsen og gælde for hele organisationen, mens andre politikker kan vedrøre et afgrænset område eller blot et individuelt it-system. Det skal derfor defineres, hvem, ud over fx systemejere, der har ret til at definere politikker. Disse personer skal gives adgang til policy-serveren.

En stor del af de data, der behandles i kommunerne, er personhenførbare og ofte personfølsomme. Efterhånden som sagsbehandlingen automatiseres i højere grad, og der integreres til flere fagsystemer, vil der være behov for kunne udføre revision af databehandlingen over flere systemer. Det stiller krav til bedre logningsløsninger, som dels kan spænde over flere it-systemer, dels kan registrere tilstrækkelig information til en brugbar revision. Eksempelvis skal brugere kunne følges i loggen på tværs af systemer. Det stiller nye krav til, hvordan bruger-id'er defineres, eller skaber

behov for, at en anden unik nøgle, der henføres til brugeren, registreres samtidigt i loggen.

5.9 Sikre services til tværgående samarbejde

I forbindelse med kommunalreformen er det fastlagt, at kommunerne skal være hovedindgangen til det offentlige for borgere og virksomheder. Dette skaber behov for forskellige former for dialog, samarbejde og udveksling af information mellem kommunen og andre offentlige myndigheder. Sådanne tværgående samarbejder skal kunne foregå via sikre forbindelser hele vejen fra afsender til modtager. Der er behov for løsninger til kryptering af følsom information mellem forskellige informationer. Det drejer sig om at sikre forbindelse fra en server hos kommunen til en server hos anden myndighed, såvel som kryptering af de meddelelser, der udveksles via webservices, hvor transporten kan involvere flere forskellige servere. Det drejer sig også om, hvorledes brugere fra kommunen kan identificeres og autenticitetssikres i eksterne systemer. Relevante it-standarder i forbindelse hermed er OCES, SSL, WS-Security, og SAML, samt en beskrivelse af en specifik brug af standarder i en sikker punkt-til-punkt-forbindelse kaldet OIO Web Service Arkitektur⁹ model T.

5.10 Afrunding

Hvilke brugerstyringservices, der er vigtige for den enkelte kommune, bør styres af en samlet tilgang til brugerstyring, som formuleres i en række pejlemærker.

Hvordan og hvornår man vil implementere de forskellige services, kan så afgøres af pejlemærkerne sammenholdt med vurderinger af potentialerne ved indførelsen af funktionen i forhold til områderne:

- It-sikkerhed – risikominimering
- Lovmæssige krav – Overholdelse af persondataloven osv.
- Bedre service til borgere og virksomheder
- Effektivisering
 - Hensigtsmæssig administration
 - Brugervenlighed
- Flexibilitet og interoperabilitet
 - Via standardisering og integration

⁹ Læs mere om OIO Web Service Arkitektur (OWSA) på <http://www.oio.dk/arkitektur/soa/webservices/owsa>

6 Forslag til sammenlægningsaktiviteter

6.1 Generelt

I dette kapitel giver vi forslag til aktiviteter, som kan indgå i et projekt til sammenlægning af brugerstyring i de nye kommuner. Vi diskuterer aktiviteterne i forhold til konkrete eksempler fra de kommuner, vi har talt med, og kommer, hvor det er muligt, med anbefalinger om, hvad man bør gøre.

Følgende tabel giver et hurtigt overblik over de aktiviteter, vi beskriver i dette kapitel. Efterfølgende beskrives de enkelte aktiviteter mere detaljeret.

Aktivitet	Beskrivelse
Fastlæg Pejlemærker	Hvilke trin skal der til for at opnå kommunens mål omkring brugerstyring?
Fastlæg ambitionsniveau	Niveaubeskrivelser. Hvor er vi, og hvor er vi på vej hen?
Understøt Digital Signatur.	Krav til brugerstyringsløsninger i forbindelse med digital signatur.
Fastlæg organisatorisk ansvar	Hvem har ansvaret for hvad mht. brugerstyring? Få styr på processerne.
Bestem brugerinformation/sammenhænge	Hvem må få adgang til hvad?
Migreringsstrategi	Hvorledes sammenkøres brugerinformation, migreringsplan?

6.2 Fastlæg pejlemærker for brugerstyring i den nye kommune

Vi anbefaler, at man i kommunerne, som første aktivitet i sammenlægningen af de forskellige brugerstyringsystemer, udstikker en række fælles pejlemærker. Pejlemærkerne kan fx beskrive overordnede og generelle krav til brugerstyring i den nye kommune. Der refereres så tilbage til disse pejlemærker senere i forløbet, efterhånden som der skal tages mere detaljerede og implementeringsspecifikke beslutninger.

I kapitel 14 gives forslag til principper/pejlemærker for brugerstyring, som eventuelt kan anvendes som udgangspunkt for formulering af egne pejlemærker.

6.3 Fastlæg ambitionsniveau i forhold til sammenlægningsopgaven

Sammenfattende kan sammenlægningsstrategierne inddeles i følgende tre muligheder:

1. Nuværende systemer anvendes som basis.

2. Der standardiseres. Samme slags systemer anvendes til brugerstyring, samme formater for navngivning, samme datamodel for bruger etc.
3. Brugerstyringssystemerne integreres. It-understøttelsen automatiseres til håndtering af en fuld livscyklus for en it-bruger.

Hvilken strategi, man lægger sig fast på, afhænger af, hvilke krav kommunens nye forretningssystemer stiller til brugerstyringen. Desuden afhænger strategien af, hvilken økonomi og hvilke kompetencer, der er til rådighed for etablering og administration af den sammenlagte brugerstyringsløsning samt af de nuværende it-systemers modenhed. De 3 strategier kan ses som en naturlig udvikling i modenhed. Man starter med at køre videre med sine eksisterende systemer, dernæst standardiserer man, hvorefter man til sidst automatiserer.

Det kan dog siges, at fortsat drift med de eksisterende systemer generelt kun vælges for en relativt kort periode. Det vil være meget svært at understøtte sammenhængende og fleksible it-løsninger, hvis basis for brugerstyring findes i flere forskellige systemer, og det vil medføre relativt høje administrationsomkostninger.

Beskrivelserne i de følgende afsnit er derfor lavet ud fra antagelsen om, at man har valgt at standardisere eller integrere den nye brugerstyringsløsning.

6.4 Understøttelse af Digital Signatur

I dag har relativt få kommunalt ansatte behov for deres egen digitale signatur. Det drejer sig primært om ansatte med behov for adgang til funktioner i arbejdsmarkedsportalen eller undervisningsministeriets uddannelses-tilmeldingssystem. Dette er dog ved at ændre sig i forbindelse med ”Borgerservicecentre, som bl.a. skal tilgå skatte-systemer hos staten, JobCentre, hvor ansatte fra AF også skal støttes, etc.”

Til modtagelse og afsendelse af sikker e-post anvendes en organisatorisk digital signatur for hele kommunen. Administration og anvendelse af digital signatur i det nuværende niveau kræver således i en lang række kommuner ikke mange ressourcer og stiller ikke store krav til it-infrastruktur. Dette afhænger dog af kommunens størrelse, hvilket det følgende eksempel viser.

Eksempel

Ressourcebehovet i forhold til administration af digital signatur afhænger af kommunens størrelse. Store kommuner, som f.eks. Københavns kommune, bruger mange ressourcer på at anvende digital signatur. Kommuner som Egedal har et meget begrænset brug af ressourcer, og f.eks. skoleområdet klarer deres egen administration i forbindelse med f.eks. Undervisningsministeriet.

Væksten i behovene for understøttelse af digital signatur afgøres dels af kommunens egne valg og dels af samarbejdspartneres valg. Nogle eksempler på sådanne valg er:

- Indførelse af mulighed for, at individuelle medarbejdere kan kommunikere med borgere og virksomheder via sikker e-post. Dette kræver, at alle medarbejdere, som skal kunne sende sikker e-post, tildeles digital signatur med et såkaldt split-certifikat.
- Internt automatisering med elektroniske blanketter, som kan underskrives med digital signatur. Dette kræver tildeling af digital signatur til alle medarbejdere, der skal kunne anvende interne elektroniske blanketter.

- I nye eller eksisterende eksterne systemer, fx i staten, som kommunerne anvender, indføres krav om autenticitetssikring ved hjælp af digital signatur. Dette forventes i første omgang at ske for en række systemer, som kommunale medarbejdere skal benytte inden for skatte- og beskæftigelsesområdet. Det samme kan også være tilfældet i forbindelse med udveksling af sundhedsdata mellem regionerne og kommunen.

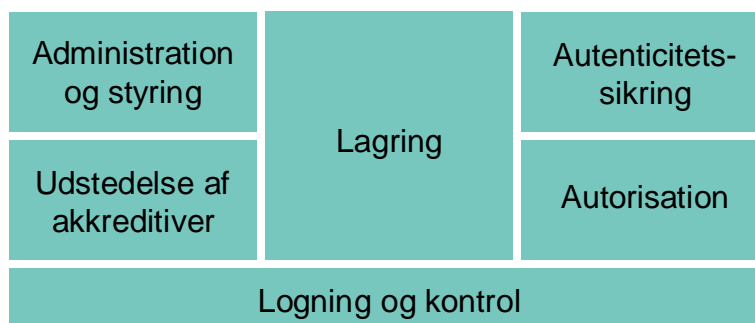
Behovet for digital signatur vokser hele tiden. Denne vækst skal der tages højde for under sammenlægningen. Et alternativ kunne være, at man allerede nu tager skridtet fuldt ud og tildeler alle ansatte digital signatur. Dette kunne så også være udgangspunkt for autenticitetssikring af brugere i kommunens interne systemer. Det anbefales derfor, at kommunerne nøje overvejer at gøre bestilling og anvendelse af digital signatur til en integreret del af det brugerstyringssystem, som sammenlægningen ender op med. Hvis det vælges at køre videre med en web-baseret løsning til bestilling af Digital Signatur, som er helt uafhængig af kommunens brugerstyring i øvrigt, kan der stille og roligt opstå en stor administrativ byrde. Dette kan også resultere i en større husholdningsopgave, når man på et senere tidspunkt integrerer bestilling og anvendelse af digital signatur med resten af brugerstyringen. i forbindelse med. Udfordringen vil her være, at få allerede bestilte digitale signaturer ind i en integreret løsning, Læs mere om mulighederne for at integrere bestilling og vedligeholdelse af digital signatur med resten af brugerstyringen i kapitel 15.

6.5 Fastlæg organisatorisk ansvar

Brugerstyringsopgaven for lokale it-systemer ligger traditionelt hos it-afdelingen/sikkerhedskoordinatoren i kommunerne, mens at den for KMD-systemerne i nogle kommuner håndteres andre steder, som fx borgmesterkontoret. Ansvar for udstedelse af digital signatur følger nogenlunde samme mønster. Men der er også eksempler på, at placering af opgaven mere er afgjort af, hvilken person, der umiddelbart havde kompetencen, end af hvilken afdeling, der rettelig burde have ansvaret. Af sikkerhedsmæssige hensyn er det hensigtsmæssigt at samle udstedelsen af akkreditiver ét sted, således at man har et samlet overblik over, hvilke akkreditiver en given ansat har fået tildelt.

Alle opgaver inden for brugerstyring behøver ikke ansvarsmæssigt at være placeret i samme organisatoriske enhed. I mange tilfælde kan it-afdelingen, som enhver anden service-leverandør, nøjes med at sørge for driften af de understøttende it-systemer, mens det forretningsmæssige ansvar for de processer, der skal udføres, kan ligge andetsteds.

Lad os betragte indledningens figur med områder inden for brugerstyring igen.



Figur 6.1. Områder inden for brugerstyring

Ansvar for processerne i de forskellige områder, der vist på figuren, kan være placeret forskellige steder, som følgende tabel giver eksempler på:

Område	Mulige placeringer af organisatorisk ansvar
Administration og styring	<p>Dette er en opgave, som it-afdelingen traditionelt varetager for de lokale it-systemer og eventuelt også for KMD-systemerne.</p> <p>Ved anvendelse af administrative systemer med tilstrækkelige workflow- og delegeringsmuligheder, kan en væsentlig del af arbejdet med administration og styring varetages af:</p> <ul style="list-style-type: none"> • Systemejerne, der definerer roller, og politikker, som bestemmer, hvem der må få adgang til deres system. • Ledelsesansvarlige, som autoriserer egne medarbejders adgang til nødvendige it-systemer.
Udstedelse af akkreditiver	<p>Akkreditiver dækker bl.a. over bruger-id og kodeord til KMD-systemer, bruger-id og kodeord til det lokale netværk, digital signatur, tokens mm. Men fx også nøgler og adgangskort til kommunens bygninger. Selv om nogle akkreditiver er fysiske ting, og forskellige teknologier anvendes til andre, er det principielt samme proces, der skal gennemgås i forbindelse med uddeling af disse. Det skal kontrolleres, at vedkommende virkelig er den han/hun giver sig ud for at være, og at vedkommende har ret til at få udleveret akkreditiverne.</p> <p>Det er værd at overveje at placere ansvaret for udstedelse (eller oprettelse) af akkreditiver et samlet sted som f.eks. personaleafdelingen, borgmesterkontoret, sikkerhedskoordinatoren eller lignende.</p> <p>Endvidere skal alle udstedelsesprocesser samt andre processer, der omhandler administration af brugere, være veldokumenteret.</p>
Lagring	<p>Processerne i forbindelse med lagring drejer sig bl.a. om at sikre, at informationen om it-brugerne er valid og konsistent. Samtidig drejer det sig også om lagring af</p>

	<p>adgangsinformationer, som forskellige it-systemer skal anvende.</p> <p>Ligesom for administration og styring kan der her blive tale om, at organisatorisk ansvar kan uddelegeres, således at fx personaleafdelingen er ansvarlig for brugernes stamdata.</p> <p>I øjeblikket er det mest oplagt, at lagring er it-afdelingens ansvar. Det skal dog ske i tæt samarbejde med personale-/løn-afdelingen og evt. med integration til deres systemer, således at basisdata om ansatte, inklusiv besked om ophør, synkroniseres.</p>
Autenticitetssikring	<p>Dette drejer sig om at sikre, at brugerens identitet er fastslået godt nok i forhold til de data og transaktioner, vedkommende skal have adgang til i et it-system.</p> <p>ikkerhedskoordinatoren bør have det procesmæssige ansvar sammen med systemejerne, mens it-afdelingen eller en serviceleverandør har ansvaret for den teknologiske understøttelse.</p>
Autorisation	<p>Hvilke services, en bruger har adgang til, afgøres dels af generelle politikker og dels af politikker inden for fagområder og individuelle it-systemer. Det bør være sikkerhedskoordinatoren, som på vegne af borgmesteren varetager ansvaret for de generelle politikker. Ansvar for politikker inden for delområder bør til gengæld tildeles relevante fagområde-chefer og systemejere. Ligesom for autenticitetssikring har it-afdelingen eller en serviceleverandør ansvaret for den teknologiske understøttelse af autorisation. Denne decentrale administration skal således understøttes af den brugerstyringsløsningsstrategi, som man ender op med at vælge</p>
Logning og kontrol	<p>Logning anvendes til en række formål, herunder blandt andet til performanceoptimering, afregning af forbrug med mere. I denne sammenhæng fokuserer vi på logning med henblik på at kunne revidere, at anvendelsen af it-systemerne sker korrekt i forhold til eksisterende lovkrav og politikker.</p> <p>Ansvar for dette bør ligge hos sikkerhedskoordinatoren.</p>

Ud af ovenstående, kan det opsummeres:

- Så vidt det teknisk kan understøttes, bør ansvar vedrørende rettigheder og administration af disse uddelegeres til systemejerne og chefer, som er personaleansvarlige for it-brugere.
- Udstedelse af akkreditiver bør samles, så én organisation varetager udstedelsen af alle akkreditiver
- Lagring af information om brugere og systemer bør organiseres, således at informationen om brugerne er den samme, som relevante dele af den basisinformation, der findes om brugerne i løn-/personalesystemet. Det bør også for de andre dele af information om en bruger klart defineres hvem, der har

forvalteransvar og opdateringsret for hver enkelt del. Dette beskrives mere detaljeret i næste aktivitet.

- Overordnet ansvar for processerne i forbindelse med autenticitetssikring, autorisation og logning/kontrol bør varetages af sikkerhedskoordinatoren på vegne af borgmesteren.
- Den tekniske understøttelse af alle områderne bør varetages af it-afdelingen eller en serviceleverandør.

6.6 Bestem hvilken information om brugere, der skal kunne anvendes i forskellige sammenhænge

Forskellig information om brugere lagres i forskellige kataloger og databaser. Det er vigtigt at finde ud af, hvilke data om en bruger, der anvendes i flere forskellige it-systemer, og sikre, at disse data opdateres ét sted, men ikke i andre it-systemer, hvor data også anvendes.

1. Kortlæg hvilke it-systemer, der lagrer brugerinformation.
2. Bestem hvem der har "forvalter-ansvar" for de enkelte dele af informationen.
3. Bestem hvor de enkelte dele af brugerinformationen skal skabes og opdateres, fx med dele i personale/løn-system, dele i brugerkatalog, dele i intranet profil-database, dele i en såkaldt attribut-service etc. Sats på at brugerinformationerne kan lagres så få steder som muligt, men forvent ikke at kunne danne ét katalog med al information om medarbejderen/it-brugeren
4. Bestem om og hvorledes brugerdata, som anvendes flere steder, synkroniseres fra it-systemet med de *sande data* til it-systemerne med kopi-data. Dette vil normalt kræve en form for integration imellem it-systemerne. Det er også en mulighed at foretage synkroniseringen manuelt, hvis det er sjældent, at data opdateres. En anden mulighed er at undlade synkronisering. Dette kan være relevant, hvis det konstateres, at det ikke er kritisk, hvorvidt visse bruger-informationer er opdaterede.
5. Bestem hvilken nøgle, der skal anvendes til at knytte bruger-informationen sammen på tværs af databaser. Denne nøgle bør også kunne anvendes til synkronisering med eksterne databaser, fx i forbindelse styring af rettigheder i fælleskommunale/regionale/statslige løsninger.

6.7 Migrering af kataloger

Selve migreringen af de kommunale it-systemer skal planlægges i god tid. Vi vurderer, at sammenlægning af kataloger er en af de mest kritiske og tidskrævende processer i kommunesammenlægningen, og behandler den derfor her separat. Sammenlægningen er kritisk, fordi samkøring af kataloger påvirker kernen i kommunernes it-infrastruktur. Opstår der problemer her, vil det påvirke stort set samtlige funktioner i kommunen. Og hvis man ikke tænker sig godt om fra starten, kommer man til at betale for det på sigt i forbindelse med komplekse oprydningsrutiner med øget administrationsomkostninger til følge.

En absolut forudsætning for en succesfuld migrering er en migreringsplan. Hvad er det, man ønsker at opnå, og hvad er målet med sammenlægningen? Hvorledes skal den

implementeres, herunder også tidsplan og fallback strategi. Hvad er et 'must' og hvad er 'nice to have'?

Har man 2 kommuner med hvert deres katalog, er der umiddelbart tre muligheder for sammenlægning:

1. Man kører videre på den eksisterende struktur og opretter en form for trust (forbindelse, der stoles på) mellem de 2 eksisterende domæner.
2. Man migrerer data fra det ene katalog over i det andet katalog og benytter dette som master-katalog.
3. Man migrerer begge kataloger op i et nyt, samlet katalog..

Risikoen ved migreringen er, for selve migreringshandlingen, mindst ved pkt. 1 og størst ved pkt. 3. Punkt 3 har den fordel, at man får chancen for at 'rydde op'.

Før en migrering skal man danne sig et overblik over sine katalogdata. Hvilke data har man, og hvilke data, herunder også skemadefinitioner, ønsker man i den nye struktur? Hvilke attributter kan udelades, og hvilke skal føres med?

Eventuelle navnesammenfald skal ryddes op inden migreringen. Generelt kan det siges, at alle fejl, der kan undgås ved planlægning, skal prioriteres som oprydningsaktiviteter inden sammenlægning.

Det anbefales, at man foretager testmigreringer. Det sikrer, at man kender tidshorizonten for en migrering, dvs. i hvor lang tid brugerne ikke vil have adgang til it-systemerne. Endvidere kan man forberede sætte brugerne på arbejds konsekvenser. En sammenlægning afføder støj, og den skal minimeres.

6.8 Stikord til aktivitetsbeskrivelserne

Nedenstående stikord udgør ikke en komplet liste.

Bemærk også at listen indeholder aktiviteter, som fx strategi for mobile klienter, der ikke er yderligere beskrevet i denne version af vejledningen.

- Lav en strategi for brug af Digital Signatur.
 - Administration, samtænkning med øvrig brugerstyring
- Lav en strategi for understøttelse af mobile klienter.
 - PDA, Smartphones mm. til omsorgsløsninger, kontrolopgaver etc.
- Overvej brugerstyringsbehov vedrørende instant messaging, e-møder, e-learning etc.
- Lav en strategi for integration & fleksibilitet.
 - Konsolidering versus best-of-breed
 - Leverandør-standarder versus åbne standarder
- Beslut, hvorledes dokumentationen af organisationsstrukturen skal vedligeholdes.
 - Hvilke systemer har brug for at kende den?
- Lav en strategi for rolle-baseret adgangskontrol.
- Lav en migreringsplan for migrering af kataloger.
- Planlæg Directory.

- Bestem struktur i Directory: Flad, forvaltningsbestemt, funktionsbestemt, administrationsbestemt, geografisk eller ...? Bestem schema i directory. Dette omhandles kort i kapitel 11.
 - Fastlæg formater for bruger-id, e-mail-adresse, DisplayName, etc. og fokuser på semantik.
- Beslut hvor fleksible brugerstyringsprocesserne skal være.
 - Hvor meget af følgende skal kunne understøttes: Decentral, Central, Outsourcet administration.
- Beskriv brugerstyringsprocesserne.
 - Beslut hvor høj grad af automatisering, der ønskes i brugerstyringen.
 - Password-synkronisering, Meta-Directory, Link til Personale-/løn-system, Provisioneringsløsning, integration med bestilling af fysisk adgangskort, IP-telefoni etc.
- Vælg/anskaf teknisk løsning.
 - Ud fra beskrevne krav, herunder krav med henblik på fællesoffentlig interoperabilitet.

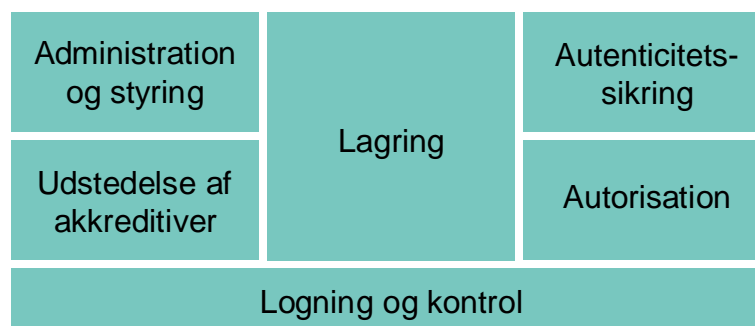
7 Rammesystemer

7.1 Introduktion

Kommunen står over for udfordringerne med at sammenlægge deres brugere i kataloger. Men hvorledes skal dette foregå, og hvorledes skal driften fortsætte efter sammenlægningen. Kan man investere i produkter, som kan gøre den daglige administration lettere for den enkelte kommune. Dette afsnit beskriver kort mulighederne for at anvende rammesystemer, dvs. systemer, der dækker et bredt spektrum af de behov, administratorer og it-ansvarlige har i forbindelse med administration af kataloger.

7.2 Generelt

Lad os igen betragte figur 1 fra kapitel 2, som viser områder inden for brugerstyring:



Figur 2.1. Områder inden for brugerstyring

Vi taler om et rammesystem i forbindelse med brugerstyring, når en enkeltstående applikation eller en suite af applikationer, der er udviklet til at fungere som en enhed, kan løse brugerstyringsområderne; enten helt eller delvist. Dette forstået som administration af katalog (struktur, indhold), understøttelse af arbejdsprocesser, selvbetjening etc.

Et rammesystem, som vil være relevant for en kommune, bør kunne leve op til og understøtte de behov, der blev defineret i kapitel 5 og opremset nedenfor:

- SSO, Simplificeret Sign-On.
- Nulstilling af kodeord.
- Mere effektiv brugeradministration og selvbetjening, herunder også administration af egne brugeres rettigheder i eksterne løsninger.
 - Standardiseret logning og kontrol
 - Sporbarhed i forbindelse med revision
 - Historik på brugeradministrationen
 - Standardisering af bruger-id'er
- Anvendelse af digital signatur (OCES) til kryptering, signering og uafviselighed for alle it-brugere.
- Sammenhæng mellem brugerkataloger og "telefonbogsservice", som ud over kontaktinfo også dækker kompetencer, interesser, og organisatorisk ophæng (Directory-services).
- Samlet provisionering ved brugeroprettelse og workflow.

- Styring af politikker.
- Sikre services til tværgående samarbejde (udveksling af data, tilgang til services etc.).

Listen kan ses som en opsummering af de arbejdsopgaver, der i dag er med til at administrere brugere i kommunerne. Her foregår det i stor udstrækning via manuelle arbejdsgange.

De store systemleverandører¹⁰ som IBM, Oracle, Microsoft mm. kan alle tilbyde en suite af produkter inden for brugerstyring. Det er vores opfattelse, at der ikke eksisterer et produkt, der kan løse alle udfordringerne på én gang, men at man må sammensætte en produktportefølje for at få opfyldt sine behov. Man kan endvidere sige, at valget af it-infrastruktur begrænser udvalget af applikationer, der understøtter netop den løsning, man har behov for.

Inden man vælger et rammesystem, er det vigtigt, at man nøje specificerer de områder fra brugerstyring, man ønsker dækket. Skal systemet være en applikation, der bygger på et katalog, eller skal systemet i sig selv indeholde et katalog? Er der løse grænseflader til kataloget, eller bygger systemet på en proprietær teknologi? Hvordan skal opgraderinger håndteres? Og hvorledes fungerer systemet sammen med eksisterende løsninger? Skal der være mulighed for decentral administration mm.? Mange andre spørgsmål vil opstå og skal besvares, inden man kan tage stilling til, om et givet rammesystem er vejen frem.

Specielt i forbindelse med kommunalreformen vil mange kommuner skulle igennem en modningsfase af deres brugerstyringsapplikationer. Der vil ske en del oprydning af eksisterende brugere og organisationsstrukturer, inden man kan betragte brugerstyringen som værende i en stabil fase.

Dette skal ikke forstås således, at det ikke er muligt at investere i rammesystemer til understøttelse af brugerstyringsproblematikken i den nuværende modningsfase. Det er bare vigtigt, at man har et stabilt udgangspunkt, da man ellers på sigt vil skulle investere i yderligere ressourcer i forbindelse med reorganisering af sin it-infrastruktur. Det er her vigtigt at pointere, at vedligeholdelse og drift af it-systemer er omkostningstungt. Det er derfor vigtigt, at man sikrer en fornuftig infrastruktur, da dette ligeledes påvirker de driftsomkostninger, man får på sigt.

¹⁰ Her er en liste med eksempler på leverandører af rammesystemer til brugerstyring. Listen er ikke fuldkommen:

Computer Associates International, Inc
 IBM
 Microsoft Corporation
 Novell, Inc.
 Oracle Corporation
 Siemens AG
 Sun Microsystems, inc

8 Fastlæggelse af ambitionsniveau og faser

8.1 Introduktion

En organisation kan være mere eller mindre klar til forandringer. Man kan her tale om modenhed af den enkelte organisation i forhold til forandringen. Store forandringer vil typisk kræve en organisation, som er gearret til de forandringer, der kommer til at ske for at forandringsprocessen kan blive en succes. I dette dokument taler vi om modenhedsfaser.

Det er vigtigt, at man, selvom der kan være lang vej, hele tiden holder sig for øje: Hvor er det, vi er på vej hen? De valg, man foretager tidligt i forandringsprocessen, kan blive af afgørende betydning for, om man når sit endelige mål.

8.2 Modenhedsfaser

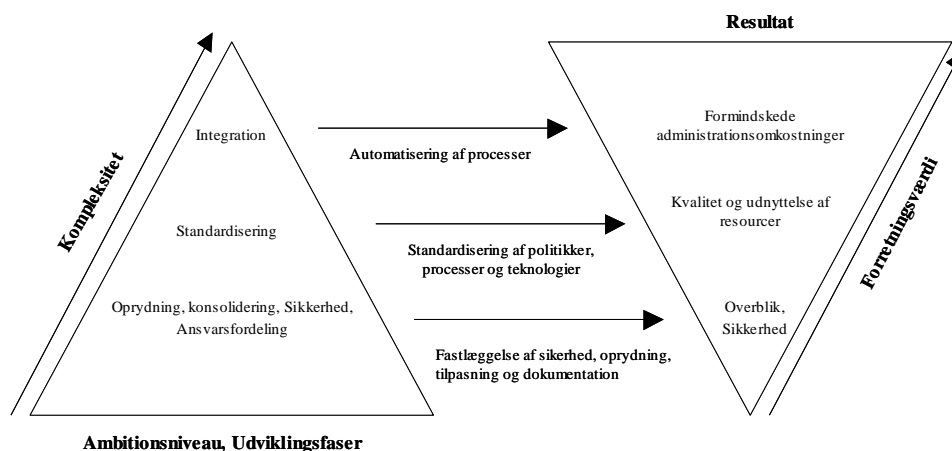
8.2.1 Overlev, Standardiser eller Integrer?

Som der blev nævnt i forrige kapitel, vil mange kommuner skulle igennem en 'modningsfase' i forbindelse med kommunalreformen.

Ønskepositionen er, at den nye kommune har tid og fuldt overblik til at lave en ny infrastruktur for brugerstyring, der overholder alle standarder, som er løst koblet, og som understøtter fremtidige udviklingstendenser inden for brugerstyring og interoperabilitet.

Realistisk set er det de færreste kommuner, der når til denne 'rene' tilstand inden d. 1. januar, 2007, og det er derfor nødvendigt, at den enkelte kommune gør sig bevidst om sit modenhedsstadium. Er man klar til at investere i ny software i forbindelse med brugerstyring, eller skal man først og fremmest satse på at konsolidere eksisterende løsninger og data, inden man investerer? Skal man køre videre med eksisterende løsninger, eller er der behov for nye? Er de data, man har, af ordentlig kvalitet, eller skal der ske en revidering/oprydning?

Udviklingen i modenhed kan beskrives som værende opdelt i forskellige faser som figuren nedenfor illustrerer.



Første fase

Første fase koncentrerer sig om konsolidering af eksisterende løsninger.

Der er fokus på grundlæggende byggeklodser som data, sikkerhed og administration. Data skal ryddes op, så der ikke er gamle og redundante data i systemerne. Endvidere skal man have sikret sig, at man har dokumenteret sine data: Hvad ligger hvor, og hvordan er relationerne mellem de forskellige datakilder? Har man datamodeller? Hvorledes administreres data? osv.

Ved at få overblik over data, samt evt. ryddet op i redundante data, sikrer man sig et godt udgangspunkt for at kunne optimere sine processer. Man sikrer sig desuden, at kvaliteten af ens datagrundlag stiger. Data er det vigtigste fundament i alle systemer. Grundlæggende sikkerhed drejer sig i grove træk om at beskytte sine data. Det drejer sig dels om fysisk beskyttelse – hvad vil ske, hvis man mister det system som indeholder data? Kan man genskabe sine data? Vil man miste data, fx fra sidste backup til nedbrud? Har man råd til at miste data?

Og så handler det om adgang til data – hvorledes sikres det, at uvedkommende ikke får adgang til data?

I denne fase vil man formodentlig køre videre på et eksisterende system, der så at sige tilpasses de nye omgivelser. Den funktionalitet, der understøttes, er arvet fra en eksisterende struktur. Den betyder, at man ved, at man har en løsning, der kan køre og fungere. Måske fungerer den ikke optimalt, men den kører. Dvs. man overlever – men heller ikke mere.

Anden fase

Anden fase drejer sig om standardisering af begreber, politikker, procedurer og, ikke mindst, teknologier. Også her er dokumentation af data, processer etc. et centralt emne. Udveksling af data og information på tværs af systemer gøres væsentligt lettere, hvis man taler samme sprog og har fælles forståelse af begreber. På dette niveau skal man derfor også diskutere semantik, dvs. betydning og fortolkning af felter.

Fordelene ved en fælles begrebsforståelse er store. Modtager man f.eks. et navn fra et system, vil man kunne anvende det direkte, fordi spillereglerne allerede er aftalt. Man ved således, hvorledes feltet er opbygget. Et personnavn vil f.eks. kunne skrives som fornavn, efternavn eller efternavn, fornavn.

Har man en fælles begrebsforståelse bliver det nemmere at stille krav til nye leverandører. Spillereglerne er jo defineret på forhånd, hvilket vil sige, at en del af kravspecifikationen til nye systemer er givet på forhånd.

Tredje fase

Tredje fase handler om integration og automatisering. Konsolidering og standardisering danner fundament for at automatisere processer. Fælles begrebsforståelse gør, at data kan bevæge sig uden at skulle konverteres. Objekterne og deres indhold er specificeret og kendt. Man benytter således fælles semantik. På dette niveau giver det mening at tale om rammesystemer og workflow-systemer, som er fuld integreret. Provisionering af data er på dette niveau let, idet standardisering sikrer interoperabilitet.

De fleste kommuner vil kunne argumentere for at have systemer/processer, der hører til hver af de tre faser. Man kan således ikke tale om en ren faseopdeling. Ideen er, at den enkelte kommune skal overveje og analysere sin egen situation. Og når der træffes beslutninger, så sker det med henblik på, at man i fremtiden gerne vil nærme sig fase 3. Man skal så at sige fremtidssikre sine investeringer.

9 anbefalinger vedrørende format på bruger-id

9.1 Generelt

Oprettelse af it-brugere hos kommunerne sker i dag uden en fælles kommunal standard. Man har en KMD's ramme (men ikke standard) for bruger-id, som hovedsaglig anvendes til KMD's systemer. Hver kommune har typisk sin måde at navngive sine it-brugere på. I nogle kommuner benyttes initialer, mens man i andre kommuner også har eksempelvis en afdelingskode med, ud over initialerne.

I forbindelse med kommunalreformen vil de fleste kommuner skulle ud og give deres brugere nye bruger-id'er for at undgå navnesammenfald.

Hvilket format den enkelte kommune vil anvende for sine bruger-id'er vil sandsynligvis afhænge af forskellige præferencer, indarbejdede formater etc. Vi ser ikke de store interoperabilitetsfordele ved en anbefaling om en fælles standard for bruger-id, ud over for digital signatur, og ser således ingen fordel i at anbefale kommunerne et bestemt format for bruger-id'er.

Der er dog nogle sikkerhedsmæssige overvejelser, som vi anbefaler, at kommunen gør sig, når det nye bruger-id-format fastlægges. It-sikkerhedsstandard DS484:2005 stiller nogle krav til indholdet af et bruger-id. Der er krav om, at alle statslige organisationer skal anvende DS484-standard, og amterne er også begyndt på indførelse af standarden. Der er i dag intet krav om at kommunerne skal følge DS484, men kommunerne bør overveje om det senere kan komme som en fælles beslutning eller et krav. Hvis det format for bruger-id som vælges i forbindelse med kommunalreformen ikke overholder DS484 kan det senere resultere i en dyr konvertering af bruger-id'er i forbindelse med overholdelse af DS484.

For eksempel har anvendelsen af initialer til bruger-id et sikkerhedsproblem. Initialer kan relativt nemt gættes og derved vil en eventuel hacker kun skulle gætte password. DS484 introducerer et ekstra sikkerhedslag ved ikke at benytte bruger-id, der er lette at gætte,

I den forbindelse vil det efterfølgende afsnit give en vejledning i, hvorledes der kan laves bruger-id, som opfylder kravene i DS484 vedrørende bruger-id.

Bemærk, at man, ved at anvende regler som f.eks. skiftevis anvendelse af hhv. vokaler og konsonanter kan gøre et bruger-id nemmere at huske, netop fordi det kan udtales. Vi omtaler dette som en fonetisk overvejelse.

Man kan argumentere for, at brugere ikke vil kunne huske et vilkårligt bruger-id og derfor alligevel skrive det ned fx på en gul seddel, som ligger frit tilgængelig. Så har man rent sikkerhedsmæssigt ikke opnået noget. Men ved udbredelse af SSO vil antallet af bruger-id'er kunne begrænses, hvilket retfærdiggør, at man bør kunne huske sit bruger-id – man har jo kun ét (og de fleste kan f.eks. huske deres telefonnr.).

9.2 Bruger ID

Valget af en navnestandard er en af de væsentligste beslutninger, der skal træffes for at sikre en korrekt implementering af et brugerkatalog.

Valget af navnestandard er ikke et valg mellem flere standarder, men udelukkende et valg af, at man vil følge nogle enkelte grundprincipper, som ikke kan eller må fraviges.

Udgangspunktet er de retningslinier, som opstilles af ESDH projektet, ”bedste praksis”, herunder DS484 vedrørende navnestandard. Her er et eksempel på, hvilke retningslinier det kan resultere i:

1. Alle bruger-id skal være unikke inden for den enkelte organisation.
2. Alle brugere i organisationen får et bruger-id, som er forskelligt fra e-post id’et.
3. Alle brugere i organisationen tildeles et bruger-id, der sammensættes af minimum 6 tegn, som indeholder både bogstaver og tal, og som er uden sammenhæng med brugerens organisatoriske tilhørsforhold¹¹.
4. Ingen bruger-id, der har været tildelt en bruger før, genbruges¹².
5. Der skelnes mellem store og små bogstaver.

Der skelnes dog IKKE mellem store og små bogstaver ved undersøgelse af genbrug.

Det er op til den enkelte organisation at sikre, at det enkelte bruger-id på et senere tidspunkt kan kobles sammen med et ansættelsesforhold eller en person.¹³

Eksempel 9.1

En kommune skal oprette en ny bruger i brugerkataloget.

Brugeren tildeles bruger-id’et g020G5.

Brugeren skal anvende g020G5 og ikke f.eks. G020g5 jf. pkt. 5 ovenfor.

g020G5 blokerer for en ny bruger med et id som f.eks. G020G5 jf. pkt. 6 ovenfor.

Ovenstående indstilling tager ikke udgangspunkt i en international standard for oprettelse af et bruger-id, men i ’ bedste praksis’. Dette skyldes, at en bruger-id-standard ikke findes.

En alternativ strategi kan være, at man anvender KMD-rammen for bruger-id’er. Dette fordrer dog, at der ud over kommunenummeret ikke lægges andre betydende ting (som fx hvilken organisation man sidder i) ind i KMD-bruger-id’et.

¹¹ Dette er i henhold til DS484. Man kan i dag via self-service applikationer hurtig få adgang til brugeres organisatoriske tilhørsforhold ved opslag. Denne information ses derfor ikke længere nødvendig som en del af et bruger-id.

¹² Genbrug er et problem, idet man kan risikere, at en ny bruger med samme bruger-id får tilknyttet for mange rettigheder. F.eks. vil man i et omsorgssystem kunne oprette en ny ’genbrugsbruger’ ved udelukkende at tildele denne en ny adgangskode. Brugeren eksisterer allerede i systemet. Den nye bruger vil således opnå sammen rettigheder som den gamle bruger.

¹³ Generelt kan man også nævne, at anvendelse af initialer i bruger-id’et ikke er hensigtsmæssig. Initialer kan skifte i forbindelse med at man bliver gift/skilt, og det skal tilsigtes, at levetiden af et bruger-id skal dække over hele ansættelsesforholdet.

Herved vil en bruger kun skulle huske dette bruger-id, og det er entydigt på tværs af kommuner.

Af hensyn til evt. gamle systemer, hvor bruger-id'et skal anvendes, bør man overveje længden af sit bruger-id. Der findes systemer, som ikke kan håndtere mere end 6 karakterer. Dette skal undersøges, før der defineres en bruger-id standard. Selvom man har sådanne gamle systemer, behøver man dog ikke at begrænse sin nye standard tilsvarende. Man kan blot beslutte at køre videre med andre bruger-id på de gamle systemer, hvis de ikke anvendes i udstrakt grad, eller hvis det planlægges at udfase dem på sigt.

10 Anbefalinger vedrørende basis datamodel for bruger

10.1 Definition af bruger

Et helt centralt element i kommunernes it-infrastruktur er definitionen af en bruger. Hvorledes kendetegnes en bruger? Alt efter hvilken kommune, man spørger, vil opfattelsen af, hvilke attributter, der kendetegner en bruger, være forskellig. F.eks. vil ikke alle kommuner opfatte en adresse som nødvendig at gemme i et brugerkatalog. Nogle vil mene, at adressen er med til at identificere brugeren og derfor er en væsentlig attribut, der skal gemmes sammen med brugeren uanset placering. Det afhænger også af, hvilke funktionaliteter/tjenester, man ønsker, at kataloget skal understøtte. Hvis man ønsker at trække adresselister, er det hensigtsmæssigt med adresseoplysninger. Men hvis disse lister trækkes fra et personalesystem, er adressen måske ikke så vigtig i brugerkataloget.

Ovenstående giver udfordringer i forbindelse med udveksling af brugerinformation mellem kataloger – både internt og eksternt. Fysisk sammenlægning af kataloger eller oprettelse af meta-kataloger med brugerinformation bliver således en større udfordring pga. de forskelligheder, der hersker.

For at illustrere dette tager vi lige fat i adresse-eksemplet igen. En adresse hører til personen og bør derfor gemmes i personalesystemet. Eller skal personalesystemet trække adressedata fra brugerkataloget? Eller har personalesystemet sit eget katalog som synkroniseres med de øvrige kataloger? Eller der er måske slet ingen synkronisering? Og hvis personalesystemet gemmer adressen, hvorledes sikres det så, at det er den adresse, som de øvrige kataloger lagrer og benytter?

Brugerdatamodel – LDAP ver. 3.0

Det giver ikke mening at lave en komplet liste med attributter, som man skal have med i sit brugerkatalog. Som beskrevet ovenfor vil anvendelse af et brugerkatalog afvige meget fra kommune til kommune. Dermed afviger også behovet for data, der gemmes i kataloget.

Til gengæld giver det mening, at alle bruger de samme standarder mht. navngivning samt formater internt som eksternt. Hvis to kataloger skal udveksle information om en bruger, er det en forudsætning, at de taler samme sprog. Endvidere er det en stor fordel, hvis navne og formater på de oplysninger, der udveksles, er identiske. Til dette er det den fællesoffentlige anbefaling at anvende standarden LDAP, ver. 3.0.

Fællesoffentligt anbefales også et minimumsset af attributter, der som udgangspunkt skal med. Disse attributter betragtes som nødvendige, for at et brugerobjekt har betydning:

Basisattributter:

- | | |
|--------|--|
| • sn | Efternavn |
| • cn | Navn – det som personen omtaler sig som. |
| • uid | Bruger-id |
| • mail | Mailadresse |

Nye attributter, som ikke er defineret i eksisterende LDAP, ver. 3.0 objektklasser

- uniqueAccountKey Id-nøgle til matchning og synkronisering af brugerinformation på tværs af systemer.
- cvrNumber CVR nummer. Angiver brugerens ansættelsesmæssige tilknytningsforhold¹⁴.

'uniqueAccountKey' og 'cvrNumber' er ikke obligatoriske. 'uniqueAccountKey' skal kun angives i de tilfælde, hvor man har valgt at implementere en unik nøgle i sit system. Høringsdokumentet 'Anbefaling om unik Id-nøgle'¹⁵ anbefaler, hvorledes den enkelte organisation kan oprette en nøgle, der er unik på tværs af organisationer.

Bemærk, at organisatorisk tilhørsforhold ikke er taget med. I forbindelse med kommunernes anvendelse af kataloger vil det dog være en oplagt attribut at medtage, idet de kommuner, vi har kendskab til, alle organiserer deres brugere efter organisatoriske tilhørsforhold. Anvendelse af ou-attributten følger naturligt, hvis man organiserer sit LDAP-træ efter organisatoriske enheder.

Eksempel:

Katalog A: Bruger-id gemmes i attributten user-adgangs-Id og kan indeholde 8 alfanumeriske tegn

Endvidere har man et felt: User-Id, der ikke umiddelbart benyttes, og som kan indeholder 32 alfanumeriske tegn

Katalog B: Bruger-id hedder uID og kan indeholde 32 alfanumeriske tegn.

Hvis brugeroplysninger skal overføres fra katalog B til katalog A har man en udfordring. Er betydningen af feltet nu det samme? Hvad nu hvis uID er 10 langt?

Hvordan mappes data egentlig, når attributnavnene er forskellige?

I LDAP-schemaet inetOrgPerson gemmes bruger-id i feltet 'uid'.

Som eksemplet viser, vil en fælles standard for at gemme og navngive brugere have sin berettigelse.. I høringsdokumentet 'Anbefaling til Kerneattributter for Bruger' anbefales det som udgangspunkt at anvende attributter, der har sin oprindelse fra LDAP, ver. 3 (og mere konkret: LDAP schemaet inetOrgPerson), hvor det er muligt. Dette er veldefinerede standardattributter, der anvendes internationalt. Det betyder, at beskrivelse og format af de enkelte attributter ligger fast. Derved vil en overførsel af data fra et brugerkatalog til et andet blive gjort betydeligt lettere, i og med at data ikke først skal 'oversættes'.

To kataloger, der begge anvender schemaet 'inetOrgPerson' til at gemme brugeroplysninger i, vil direkte kunne overføre brugerobjekter indbyrdes. Det vil selvfølgelig stadig være en udfordring, hvis der mangler data i attributter i forhold til forskellige brugerdatabaser. Men overførsel af objektet er standard, og det er afgørende i forbindelse med interoperabilitet.

¹⁴Bemærk, at dokumentet 'Anbefaling om unik Id-nøgle' også anvender CVR-nummer, men dette ikke nødvendigvis er det samme CVR nummer som her. I den anbefalede id-nøgle anvendes et CVR nummer, som hører til den institution, der oprettede brugeren i brugerkataloget. Her er der tale om det nuværende tilhørsforhold, som kan være ændret f.eks. efter en opgaveflytning mellem myndigheder.

¹⁵ Høringsdokumenter findes på <http://www.oio.dk/arkitektur/brugerstyring> under *Høringer*

En anden fordel er udvikling af nye systemer, der trækker på services/data fra kataloget. De kan drage fordel af et kendt interface og veldefinerede attributter.

Bemærk, at der i forbindelse med FESD standardiseringsarbejdet er udarbejdet standarder for brugeradministration og adressemodel. Disse standarder kan benyttes til at identificere nødvendige attributter for en bruger i et katalog i forbindelse med oprettelse af en brugermodel. Standardiseringsarbejdet begrænser ikke brugen af LDAP, men indeholder nogle overvejelser, der skal tages i betragtning. F.eks. restriktionen, at cn-attributten i FESD regi skal være mindre end 50 karakterer for at være en lovlig ESDH-bruger. Man skal således nøje overveje anvendelsen af sit katalog og evtuelle replikeringer/provisioneringer for at sikre sig, at man ikke indfører data, som er valide i én sammenhæng men invalide i en anden.

11 Katalog-struktur

11.1 Indledning

Kataloger benyttes til at lagre statisk information. I kataloger ligger data i et fast-defineret træ, hvor søgninger kan foretages hurtigere, end hvis data f.eks. lå i en relationel database. Dette anvendes ikke mindst i forbindelse med lagring af data til autenticitetssikring i forbindelse med brugerstyring.

Anbefalinger i forbindelse med katalogstruktur er meget aktuelle i forbindelse med kommunalreformen, hvor kommuner, der skal sammenlægges, vil stå over for udfordringen med at sammenkøre eksempelvis brugere. Brugere vil typisk være registreret i eksisterende kataloger, som er struktureret forskelligt fra kommune til kommune. I forbindelse med sammenlægningen vil det derfor være en stor hjælp at få lagt rammerne fast i forbindelse med sammenlægning af data. Således bliver kataloger konsistente, og data vil kunne udveksles (interoperabilitet).

Kapitlet her forudsætter kendskab til begreber inden for kataloger. Specielt benyttes terminologien fra X500/LDAP.

I det følgende vil den engelske betegnelse, directory, for et katalog blive benyttet, hvor det er fundet hensigtsmæssigt.

11.2 Generelle overvejelser

I høringsdokumentet 'Anbefaling til Kerneattributter for Bruger' anbefales anvendelse af navnestandard/attributnavne fra LDAP, version 3.0. (Se evt. også kapitel 10). Dette vil på sigt sikre, at når et system har en attribut som f.eks. uid, så vil den kunne udveksles med et andet system. Fælles begrebsforståelse åbner og er en forudsætning for interoperabilitet.

På sigt vil ét eller flere fælles nationale/regionale brugerkataloger ikke kun være en teoretisk mulighed. Et sådan katalog vil skulle fødes af lokale brugerkataloger med et prædefineret sæt af attributter, da det ikke ville være muligt for en enkelt central administration at holde dette katalog synkroniseret. En forudsætning for dette vil være en fælles begrebsforståelse. Man vil således allerede nu kunne forberede et sådant fælles katalog ved at følge ensrettede standarder.

Et centralt brugerkatalog vil kunne benyttes til autenticitetssikring af brugere i en central login-service. Det er utopi at tro, at man kan definere et fælles rollebegreb for alle brugere og alle applikationer, og det vil derfor være regelbaseret adgangskontrol, der lægges op til. Alt efter hvilken applikation, der benytter denne fælles service, vil der være behov for forskellige attributter til den regelbaserede adgangskontrol. Hvis attributterne allerede er defineret og standardiseret bliver denne opgave betydeligt lettere, end hvis man først skal til at oversætte.

Hvis roden af hvert lokale katalog endvidere er unik, så vil et centralt katalog med hvert lokale katalog som undertræ udelukkende bestå af unikke koder.

Der findes ikke en 'facit' træ-struktur. Træstrukturen afhænger af

- Hvilke data man ønsker at gemme.
- Hvem der ejer data, og hvorledes skal data administreres.
- Hvordan data er tilgængelige fra applikationer.
- Hvem der bruger data.

11.3 Generelle anbefalinger

- Fladt træ. Dette minimerer administrationsomkostninger ved ændringer.
- Data hørende til en bruger gemmes i inetOrgPerson.
- Der anvendes attributnavne (AD: Properties) fra LDAP, version 3.0 skemaet. Det sikrer fælles begrebsforståelse og interoperabilitet.
- Uid følger retningslinierne fra kapitel 10
- Der skal være historik-funktionalitet til kataloget. Det skal sikre sporbarhed ved ophør af ansættelsesforhold og senere forespørgsel på brugeridentitet.
- Øverste niveau (Top) i katalogtræet for sande LDAP-directories¹⁶ er organisation, o=DK, næste niveau er organisations-unit: ou=<domaine navn.local>. Dette kan f.eks. være egedal.local eller evt. cvr.nr.local. Begge vil sikre entydighed. At bruge domain-navnet som top i sin rene form, f.eks. egedal.dk, kan skabe problemer i visse kataloger og frarådes derfor.

Overholdes ovenstående, åbner det mulighed for, at man på sigt kan lave et centralt metakatalog, hvor data fra de enkelte kommuner replikeres direkte. Strukturen fra de enkelte kommuner kan bibeholdes idet <domain-name.local> er entydigt, og idet kommunerne selv styrer strukturen herefter.

¹⁶ Pga. andre afhængigheder vil øverste niveau i Microsoft Active Directory (AD) normalt være organisationens lokale domænenavn (fx *nykommune.local*). OBS – det er vigtigt ikke at anvende det udadvandede domæne navn, som fx *nykommune.dk* i AD-directory-strukturen, da dette kan foranledige en række konflikter i adresseringen mellem det interne og det udadvandede domæne.

12 Anbefalinger vedrørende interoperabilitet med andre myndigheders løsninger

12.1 Indledning

I august måned sendte it- og telestyrelsen 6 dokumenter i høring. De omhandlede alle brugerstyring og relaterede begreber. Disse dokumenters primære formål er at sikre interoperabilitet med andre myndigheders løsninger. Nedenfor er angivet de væsentligste anbefalinger fra disse dokumenter. De giver nogle retningslinier for, hvad den enkelte kommune skal sikre sig i forhold til deres leverandører af it-systemer i forbindelse med brugerstyring.

De 6 høringsdokumenter er:

Vejledning vedrørende niveauer af autenticitetssikring

- Anbefaling om fælles arkitektur for tværgående autenticitetssikring
- Anbefaling til kerneattributter for bruger
- Anbefaling til unik id-nøgle
- Anbefaling vedrørende brug af RBAC standard til rollebaseret adgangskontrol
- Rettighedsstyring for eksterne brugere – Diskussion af scenarier

Nedenfor er kun uddraget en lille del af det samlede materiale. Det anbefales særligt interesserede, at høringsdokumenterne læses i deres hele.

12.2 Niveauer af autenticitetssikring

Hvert trin i en autenticitetssikringsproces påvirker niveauet af sikkerhed. Fra validering af faktisk identitet til udstedelse af akkreditiver, over anvendelse af akkreditiver i et robust og sikkert system til journalisering, logning og kontrol. Ingen kæde er stærkere end det svageste led. Hvis et trin i en proces anvender et lavere niveau af autenticitetssikring end i resten af processen, kan dette trin kompromittere sikkerheden i de andre trin. En systemejer opnår det bedste niveau af autenticitetssikring via god kontrol i forbindelse med udstedelsen af akkreditiverne, anvendelse af stærke akkreditiver og robust administration (herunder en god arkiverings- og kontrolproces).

I forbindelse med implementering af et system til digital forvaltning er det systemejerens ansvar at bestemme det nødvendige niveau af autenticitetssikring for de transaktioner, som systemet inkluderer.

Autenticitetssikring har som fokus at bekræfte en brugers identitet på basis af pålideligheden af vedkommendes akkreditiver.

Et andet begreb er *Autorisation*, der på basis af politikker og tilladelser giver brugeren adgangsrettigheder efter, om vedkommende er autenticitetssikret.

Systemejere bør gennemgå de følgende trin for at fastsætte det nødvendige niveau af autenticitetssikring:

1. Udfør risikovurdering for det givne it-system.
2. Match identificerede risici med nødvendigt niveau af autenticitetssikring.
3. Vælg teknologi til autenticitetssikring.
4. Valider efter implementering, at systemet i drift har det nødvendige niveau af autenticitetssikring.

5. Revurder periodisk, om systemet har behov for opgradering af den teknologi, der er anvendt til autenticitetssikringen.

Der henvises til høringsdokumentet for en nærmere specifikation.

Specielt punkt 3 er relevant i forhold til leverandøren. Når man har valgt sit sikkerhedsniveau kan man stille det som krav til leverandøren, der så må vurdere sin løsning.

Eksempel

En offentligt ansat anvender en anden myndigheds it-system, hvilket giver vedkommende adgang til potentielt sensitiv information om borgere. Den ansatte arbejder i en bygning, som kun ansatte og autoriserede besøgende har adgang til, men transaktionerne med den anden myndigheds it-system sker over Internettet. Vedkommendes adgang til potentielt sensitiv information resulterer i moderat omfang i en risiko for kompromittering af personoplysninger, hvorfor der skal anvendes autenticitetssikring på et vist niveau.

12.3 Fælles arkitektur for tværgående autenticitetssikring

Baggrunden for anbefalingen er ønsket om at skabe en fælles tilgang til tværgående autenticitetssikring af brugere. Det sker af hensyn til sikkerhed samt for at gøre adgangen til applikationer lettere for den enkelte bruger via genbrug. En del af dette er en fælles arkitektur og begrebsforståelse. Ved en standardisering af brugerautenticitetssikring vil man ved udvikling af nye systemer kunne genbruge den eksisterende arkitektur.

Ved at anvende en eksisterende arkitektur og teknologi, vil man herigennem skabe tillid og troværdighed til brugerautenticitetssikringen i nye systemer.

Et fundament for dette er oprettelse af en service, der returnerer autenticitetssikringsdata, f.eks. vha. SAML 2.0. Disse data benyttes af services til at 'blåstemple' den/de brugere, der logger på. Denne kan betragtes som en login-service og er den service, brugeren interagerer med for at blive autenticitetssikret. Hver service er tilknyttet en eller flere autenticitetssikringsservices. Denne autenticitetssikringsservice kommunikerer direkte med services f.eks. via SAML 2.0.

Generelt anbefales det, at man stiller som krav til sine leverandører, at de er SAML 2.0 kompatible. Anvendelsen af SAML 2.0 er en forudsætning for interoperabilitet – man taler så at sige samme sprog. Og anvendelsen af SAML 2.0 er en forudsætning for, at man kan håndtere single-sign-on på et fælles niveau.

12.4 RBAC – Rollebaseret adgangskontrol

Det anbefales, at adgangsrettigheder baseres på roller og regler, således at rettigheder kun skal administreres for individuelle brugere i situationer, hvor roller og regler ikke kan anvendes.

Det anbefales, at der for systemer til administration af rollebaserede rettigheder stilles mindstekrav om, at de skal overholde RBAC¹⁷-kernens definitioner og krav i RBAC-standarden.

Det anbefales, at der ved anskaffelse eller udvikling stilles et mindstekrav om, at it-systemer, hvor det er relevant, skal understøtte rollebaseret adgangskontrol som beskrevet i RBAC-kernen af RBAC-standarden.

Baggrunden for disse anbefalinger er primært, at de kan medvirke til at nedbringe omkostninger ved administration af brugerrettigheder, forbedre sikkerheden og give basis for yderligere automatisering af it-brugerunderstøttelse og administration af rettigheder i eksterne systemer.

Hvis man vælger at basere sine løsninger på regelbaseret adgangskontrol i stedet, skal man fokusere på standarden XACML.

12.5 Andet

Derudover anbefales det generelt, at man løbende konsulterer

<http://www.oio.dk/arkitektur/brugerstyring> for at identificere de nyeste standarder og anbefalinger fra It- og Telestyrelsen.

¹⁷ Selve standarden kan købes online for et relativt lille beløb. Per 1. august 2005 kunne en PDF-version af RBAC-standarden købes online på http://www.techstreet.com/cgi-bin/detail?product_id=1151353 til en pris af 18 dollar.

13 Checklister

Nedenfor er et oplæg til relevante checklister i forbindelse med brugerstyring. Listerne er tænkt som et oplæg og ikke som endelige lister, der ikke kan modificeres. Det er op til den enkelte beslutningstager at vurdere i hvert enkelt tilfælde, om der er behov for yderligere informationer og/eller beslutninger.

Hvilken information skal indsamles til planlægning af brugerstyring:

Organisation

- Hvorledes ser organisationen ud mht. organisatoriske enheder, diagram, geografisk placering, antal medarbejdere mm.?

It-arkitektur

- Hvorledes ser it-arkitekturen ud i dag?
- Hvorledes anvendes hjemmearbejdspladser?

It-systemer

- Hvilke systemer haves/bruges internt og eksternt?
- Beskriv ejerforhold af de enkelte systemer.
- Hvilke systemer skal skiftes ud og hvilke bibeholdes?
- Hvor mange brugere er der i de enkelte systemer?
- Hvilke roller er der i de enkelte systemer?
- Hvorledes er eksisterende brugeradministration i de enkelte systemer.
- Hvilke muligheder er der for ekstern brugerstyring i det enkelte delsystem?
- Hvilke grænseflader er der i det enkelte delsystem?
- Hvilke autentifikationsmekanismer benyttes i systemerne?
- Hvilke autorisationsmekanismer benyttes i systemerne?
- Hvilke krav til bruger-id, kodeord, certifikater mm. er der i de enkelte delsystemer?
- Hvorledes bruges PDA'ere?
- Hvorledes anvendes log i de forskellige systemer?

Katalog

- Hvilke kataloger benyttes?
- Hvorledes ser katalogstrukturen ud?
- Hvilke synkroniseringer sker der mellem kataloger, mellem kataloger/systemer, mellem systemer/systemer?
- Hvorledes opdateres/administreres katalogerne, f.eks. centralt el. decentralt?
- Hvilke systemer bruger kataloget?
- Hvilke data er gemt i kataloget?
- Hvilke skemaer og attributter anvendes i kataloget?

Brugere

- Hvilke brugere er der i organisationen?
- Hvilke type brugere er der i organisationen?
- Hvordan er processen vedr. oprettelse, vedligehold og nedlæggelse af brugere?
- Hvorledes administreres brugere generelt internt/eksternt?
- Hvilke brugerdata gemmes? Og hvor gemmes de?
- Hvilke brugere har hvilke rettigheder?
- Brugernes ansættelsesforhold skal undersøges. Er der f.eks. flere ansættelsesforhold per person? Og hvorledes understøttes det?

Hvilke ting skal der analyseres, vurderes og tages stilling til:

Organisation

- Hvorledes forventes organisationen at se ud fremover – organisatoriske enheder, diagram, geografisk placering, antal medarb. Mm.?

It-arkitektur

- Hvilke ønsker er der til den fremtidige it-arkitektur?
- Hvorledes skal it-arkitekturen se ud?
- Hvilke standarder skal anvendes?
- Hvorledes udvikles brugen af hjemmearbejdspladser?

It-systemer

- Hvilke systemer haves?
- Hvorledes er den fremtidige ejerskab af systemerne?
- Hvilke brugere skal have adgang til hvilke systemer?
- Hvilke grænseflader ønskes anvendt?.
- Hvilke autentifikationsmekanismer skal benyttes?
- Hvilke autorisationsmekanismer skal benyttes?
- Hvilke krav til bruger-id, kodeord, certificater mm. skal der stilles (under hensynstages til at eksisterende systemer ikke let kan ændres.)?
- Hvorledes skal brugen af PDA'ere understøttes?
- Er der behov for automatisk log-opfølgning?

Katalog

- Hvilken katalogstruktur skal anvendes fremover?
- Hvorledes skal katalogstrukturen se ud?
- Hvorledes skal kataloget anvendes?
- Hvilke synkroniseringer skal der ske mellem kataloger, mellem kataloger/systemer, mellem systemer/systemer.
- Ønsker man at anvende meta-kataloger?
- Hvem har ejerskabet over kataloget/dele af kataloget?
- Central/decentral opdatering af katalogoplysninger?
- Hvilke data ønsker man at gemme i kataloget?

Brugere

- Hvilke brugere skal håndteres nu/på sigt (Almindelige borgere kunne være et emne for diskussion)?
- Hvilke type brugere skal håndteres?
- Hvordan skal processen vedr. oprettelse, vedligehold og nedlæggelse af brugere være?
- Hvorledes skal brugere generelt administreres internt/eksternt?
- Hvilke brugerdata skal gemmes? Hvor skal de gemmes? Skal alt ligge i kataloger, eller vil anvendelse af en database være en option?
- Hvilke brugere skal have hvilke rettigheder?
- Brugernes ansættelsesforhold – flere ansættelsesforhold per person skal understøttes.

14 Principper/Pejlemærker

14.1 Forslag til principper/pejlemærker for brugerstyring

Pejlemærker for brugerstyring kan også betragtes som generelle politikker. Følgende bør gælde for pejlemærkerne:

- Kommunikerer overordnede krav til brugerstyring baseret på forretningens behov.
- Inddrager organisationens værdier, kultur og forretningens mål.
- Udstikker mål for implementering af processer og teknik.

Nogle eksempler som inspiration til formulering af mere kommunenære pejlemærker:

- Brugerstyringsløsningen skal opbygges, så den understøtter den rette balance af it-sikkerhed, overholdelse af lovkrav, effektivitet, fleksibilitet og interoperabilitet.
- Der skal gives adgang til alle informationer og ressourcer, når brugeren har et validt formål (er autoriseret).
- Brugerstyring skal give grundlaget for sikker udveksling af data – også på tværs af organisatoriske skel, hvorfor brugerstyringen skal baseres på åbne eller anerkendte branchestandarder.
- Adgang til it-løsninger baseres på identitet (og ikke blot rolle).
- Rettigheder i it-løsninger (adgang til information og ressourcer) baseres på roller (jobfunktion), som tildeles på baggrund af forretningsregler (politikker).
- Uddelegering af rettigheder skal være mulig.
- Det skal være muligt at få et samlet overblik over, hvilke adgange og rettigheder en it-bruger har.
- Nye medarbejdere skal være tildelt nødvendige adgange på første arbejdsdag.
- Alle udstedte bruger-ID'er er under livscyklus-kontrol.
- Organisationens privacy-politik svarer til kravene i person-dataloven og forvaltningsloven.
- Det skal være muligt at anvende forskellige niveauer af autenticitets sikring, som defineret i *Vejledning vedrørende niveauer af autenticitets sikring*.¹⁸

¹⁸ Vejledningen kan hentes på www.oio.dk/arkitektur/brugerstyring/xxx

- Brugere, der er identificeret på et givent autenticitetsniveau, skal også have adgang til ressourcer, der har krav om et lavere niveau af autenticitetssikring.
- Brugerstyringsløsningen udbygges løbende. Det medfører et behov for modulær opbygning med dokumenterede og, om muligt, standard-baserede grænseflader.

15 OCES – Digital Signatur

15.1 Indledning

Digital signatur udstedes af TDC OCES CA. Dette certificeringscenter understøtter administration (oprettelse, spærring, nedlæggele) af medarbejdersignaturer. Behovet for digital signatur er voksende, og det bør overvejes, om man i kommunerne ikke allerede på nuværende tidspunkt skal integrere tildeling af et medarbejdercertifikat med den øvrige brugerstyring. Flere og flere offentlige løsninger kræver adgang via digital signatur, f.eks. told og skat og sundhedsportalen, så på sigt forventes det at blive et behov. Nedenfor er beskrevet den traditionelle løsning, hvor kommunen selv er ansvarlig for administration af medarbejdercertifikater. En alternativ løsning, baseret på TDC's Ldapter, er ligeledes beskrevet. Den sidste vil automatisk sørge for, at medarbejdercertifikater altid er synkroniserede med lokale kataloger. Dette sidste er interessant, idet det vil mindske den administrative byrde, som ellers vil følge med ved anvendelse af digital signatur.

15.2 Traditionel anvendelse af OCES certifikater

Man sørger selv for at få udstedt og afmeldt certifikater. Det sker ved en eller flere af følgende:

- En webbaseret grænseflade - TDC OCES LRA
- Upload af XML el. kommasepareret fil - TDC OCES LRA
- Direkte integration til TDC OCES CA med webservices (udvikles lokalt)

Ovenstående kræver, at der er en ansvarlig administrator til at sikre, at data er synkroniserede.

15.3 Ldapter

En Ldapter¹⁹ er en applikation, der er anvender TDC's ovenfor nævnte webservices. Den forudsætter, at kommunens katalog understøtter LDAP²⁰

En Ldapter sikrer direkte integration mellem kommunens katalog og TDC OCES CA. Denne løsning indebærer installation af Ldapter-komponenter, som hører til i virksomhedens miljø, samt en mapning af, hvorledes kommunens attributter mappes til TDC OCES CA attributter.

Det antages, at kommunerne anvender TDC OCES medarbejdersignatur. Sammen med Ldapter giver dette følgende fordele:

¹⁹ Yderligere information om ldapter [fås](#) ved henvendelse til TDC

²⁰ TDC har testet løsningen mod Microsoft Active Directory og Novell eDirectory.

- Brugere, der oprettes i kommunernes lokale katalog, og som anvender OCED medarbejdersignatur, synkroniseres automatisk med TDC OCES CA. Det betyder at de ved lokal oprettelse automatisk får udstedt en signatur.
- Når brugerne ikke længere har markering for OCES medarbejdersignatur, spærres brugerens eventuelle signatur.
- Tilsvarende sker ved lokal nedlæggelse af brugeren i directory. Dette bliver automatisk opdateret i OCES.

Fordelene ved en Ldapter er, at administrationen af medarbejdercertifikater sker automatisk på baggrund af det katalog, der foreligger lokalt.

Det anbefales, at man laver denne integration, dvs. anvender en eller anden form for Ldapter, med henblik på at minimere de administrative omkostninger ved brug af digital signatur.