>

Begrebsmodel til brugerstyring

Dette udkast til standard er i offentlig høring i perioden 12. oktober til 13. november 2009

IT- & Telestyrelsen
12. oktober 2009

>

Begrebsmodel til brugerstyring

Standarden er udarbejdet af IT- og Telestyrelsen for det fælles offentlige brugerrettighedsstyringsprojekt (FBRS).

Kontaktperson :
Projektleder Rita Lützhøft Andersen
Mailadresse: rla@itst.dk.
Direkte telefon: +45 3337 9242

Udgivet af:
IT- & Telestyrelsen

Holsteinsgade 63
2100 København Ø

Telefon: +45 3545 0000
Fax: +45 3545 0010

Publikationen kan hentes
på IT- & Telestyrelsens
hjemmeside: http://www.itst.dk

Indhold >

Forord

>

Dokumentet her beskriver en fællesoffentlig begrebsmodel for brugerstyring, som viser begreberne inden for brugerstyring og deres indbyrdes relationer. Modellen er beskrevet på et konceptuelt niveau, således at den kan danne udgangspunkt for flere forskellige implementeringer af brugerrettigheds løsninger.

Målgruppen er primært myndigheder, konsulentvirksomheder og leverandører, som indkøber, rådgiver om og leverer it-løsninger i relation til brugerrettighedsstyring.

Del A – Indledning

>

Baggrund

Dette udkast til standard er udarbejdet af IT- og Telestyrelsen for det fælles offentlige brugerrettighedsstyringsprojekt (FBRS).

Målet er en fælles overordnet begrebsmodel for udveksling af information omkring aktør, roller og organisation, som kan anvendes i forbindelse med brugerrettighedsstyring.

Modellen skal danne et fælles udgangspunkt for den fælles offentlige brugerrettighedsstyring (FBRS), som de mere detaljerede sektor begrebsmodeller kan mødes i.

Begrebsmodellen er udarbejdet med udgangspunkt i primært tre modeller:

- Konceptuel model for Aktør-Rolle-Organisation dateret 18. marts 2009.
- Model for sag og dokument området (OIO-SD). Der er taget udgangspunkt i modellens udseende medio august 2009.
- Modeller omkring Digital Sundheds arbejde med brugerrettighedsstyring.

Erfaringer fra andre umiddelbart tilgængelige brugerrettighedsmodeller er inddraget (eksempelvis ”RBAC”), men opgaven har ikke omfattet et opsøgende arbejde i relation til, hvad der måtte være af øvrige modeller på området i de forskellige myndigheder.
Dette indfanges i stedet igennem den planlagte OIO-høring.

Tilblivelsesproces

Begrebsmodellen i dette dokument er udarbejdet af Strand & Donslund i perioden medio august til ultimo september 2009.

Der har i august og primo september været afholdt afstemningsmøder i forhold til OIO-SD Organisation, Digital Sundhed og ØS ”BRL Projekt”.

Begrebsmodellen har været præsenteret i et første udkast på ”OIO-SD’s 5. workshop omkring Organisation” 8. September 2009. Kommentarer herfra blev indarbejdet og præsenteret på ”OIO-SD’s 6. workshop omkring Organisation” 22. September 2009. Kommentarer herfra er sammen med kommentarer i relation til fællesoffentlig brugerstyring indarbejdet i version 1.0

Målgruppe

Målgruppen for dette arbejde er myndigheder, konsulentvirksomheder og leverandører, som indkøber, rådgiver om og leverer it-løsninger i relation til brugerrettighedsstyring.

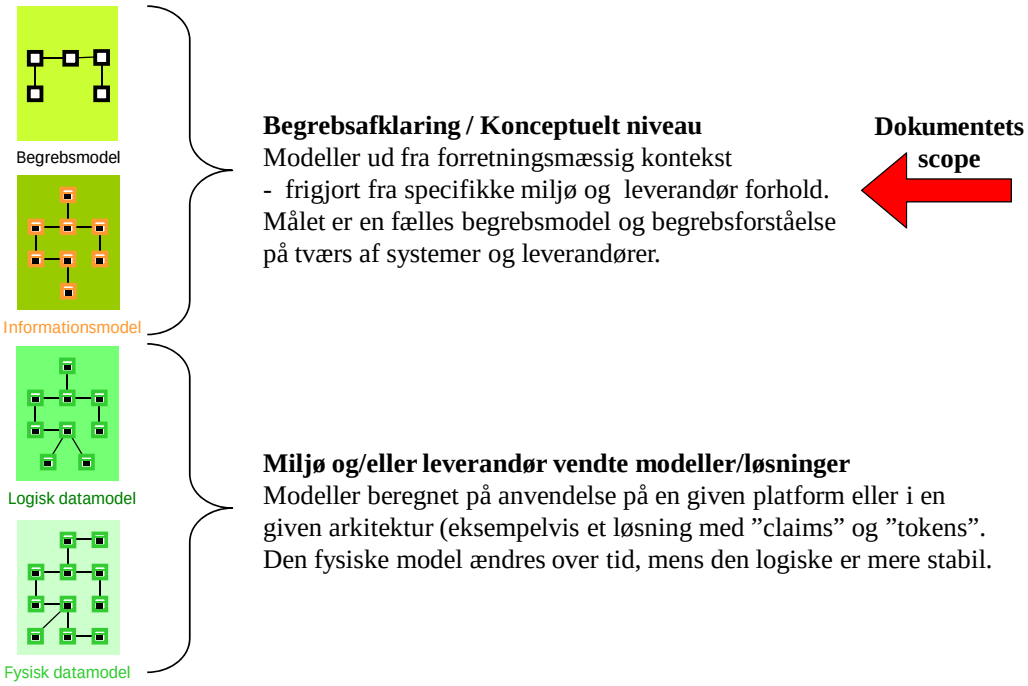
Del B – Kontekst og afgrænsning

>

Konceptuel model

Dokumentet her beskriver en fællesoffentlig begrebsmodel for brugerstyring, som viser begreberne inden for brugerstyring og deres indbyrdes relationer.

Modellen er en begrebsmodel for brugerstyringsrettigheder på konceptuelt niveau (det der på engelsk kaldes ”High Level Business Type Model”). Dvs. en model som ikke er bundet til at implementeringen skal være via claims, tokens, WS-policy, attributserver, RACF, Top Secret eller lign. Det er en model frigjort fra teknologi og platforme. Begreber, relationer m.m. er løftet til et konceptuelt niveau, således at den kan danne udgangspunkt for flere forskellige implementeringer af brugerrettigheds løsninger.

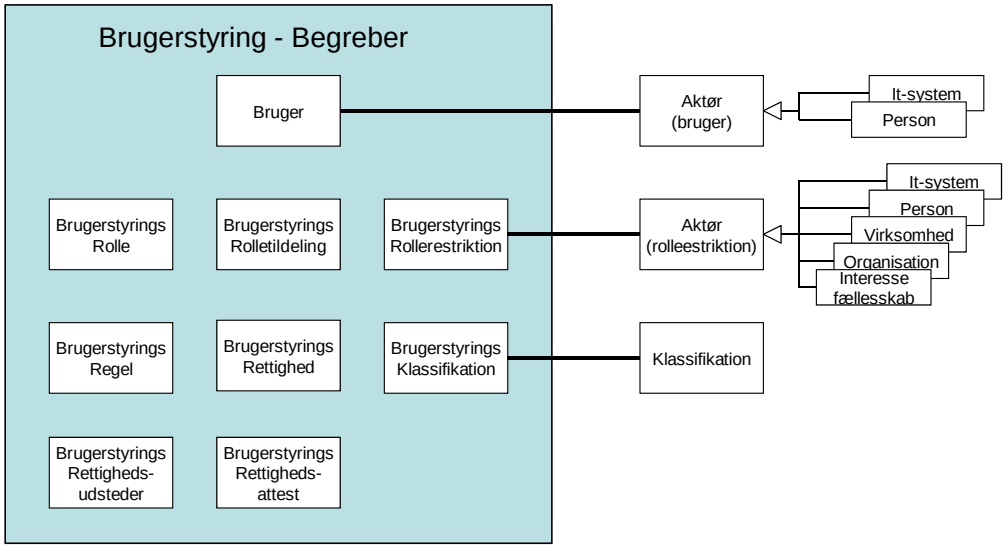


Snitflader

Der er ikke tale om en referencearkitektur for brugerstyring, hvorfor modellen kun forholder sig til eksterne begreber (eksempelvis ”Aktør”) – ikke til hvorledes disse begreber og forretningsregler opbygges i forskellige forretningsservices, ligesom den heller ikke forholder sig til, hvorledes de eksterne begreber er tænkt organiseret i forretningstjenester (eksempelvis ””Organisation” og ”Person”).

Kontekst for begrebsmodellen fremgår af nedenstående figur:

>



Der er tre væsentlige eksterne snitflader:

- Relationer til begrebet ”Aktør” i rollen som bruger.
  I modellen refererer en ”Bruger” til en aktør i rollen som et ”It-system” eller en ”Person”, hvad enten personen er en del af den offentlige organisation, fra en virksomhed eller en borger.
  En given person optræder i ”Person” som én forekomst, men kan optræde med flere forekomster i ”Bruger” – én for hvert akkreditiv.

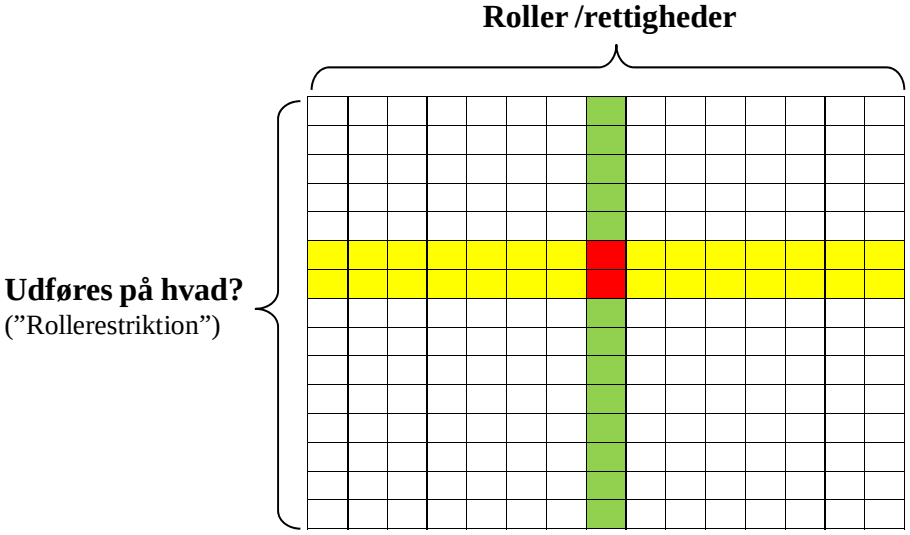
- Relationer til begrebet ”Aktør” i rollen som rollerestriktion.
  I modellen kan en rolletildeling afgrænses til kun at gælde i forhold til udvalgte aktører. Dette kan være i forhold til it-systemer, personer, virksomheder, organisationer og organisationsenheder eller interesse fællesskaber.

- Relationer til begrebet ”Klassifikation”.
  I modellen er anvendt betegnelsen ”Brugerstyringsklassifikation” for de klassifikationer, som indgår i brugerstyring.
  Brugerstyringsklassifikation er modelleret som en form for ejerskab i forhold til de forskellige roller og rettigheder.
  Formentlig kan disse klassifikationer indeholdes i det generelle klassifikationsbegreb.

>

Modelstruktur

Grundstrukturen i begrebsmodellen er bygget over en struktur svarende til nedenstående matrice:



Konceptuelt beskriver kolonnerne mængden af roller (grupper af rettigheder), som findes inden for brugerrettighedsstyring. Eksemplet kunne være rollen læge.

Rækkerne beskriver så på hvad (eller i forhold til hvad) denne rolle med tilhørende rettigheder må udføres (dette kaldes i modellen for "Rollerestriktion"). Eksemplet her kunne tilsvarende være en restriktion i forhold til, at rollen læge kun kan udføres i afdeling 101 og 102.

Tildelingen i "matricen" kaldes i modellen for "Rolletildeling" og er dokumenteret gennem en "Attest" udstedt af en "Udsteder".

De enkelte roller og rettigheder anvendes inden for forskellige klassifikationer, hvilket betyder, at der både kan være fællesoffentlige roller/rettigheder og specifikke roller/rettigheder inden for fagområder, organisationer, it-systemer etc.

Til de enkelte rettigheder kan der knyttes forskellige regler. Eksempelvis en regel om at man ikke samtidig kan have rettighed som bestiller og som godkender.

Bemærk at modellen er en konceptuel model. De enkelte rolletildelinger m.m. kan i en given implementering sagtens være noget som tildeles dynamisk ud fra informationer hentet andre steder, som man i den givne situation har tillid til. Eksempelvis ved at man gennem sin organisatoriske placering er tildelt nogle givne arbejdsfunktioner.

Del C – Begrebsmodel

>

Overblik

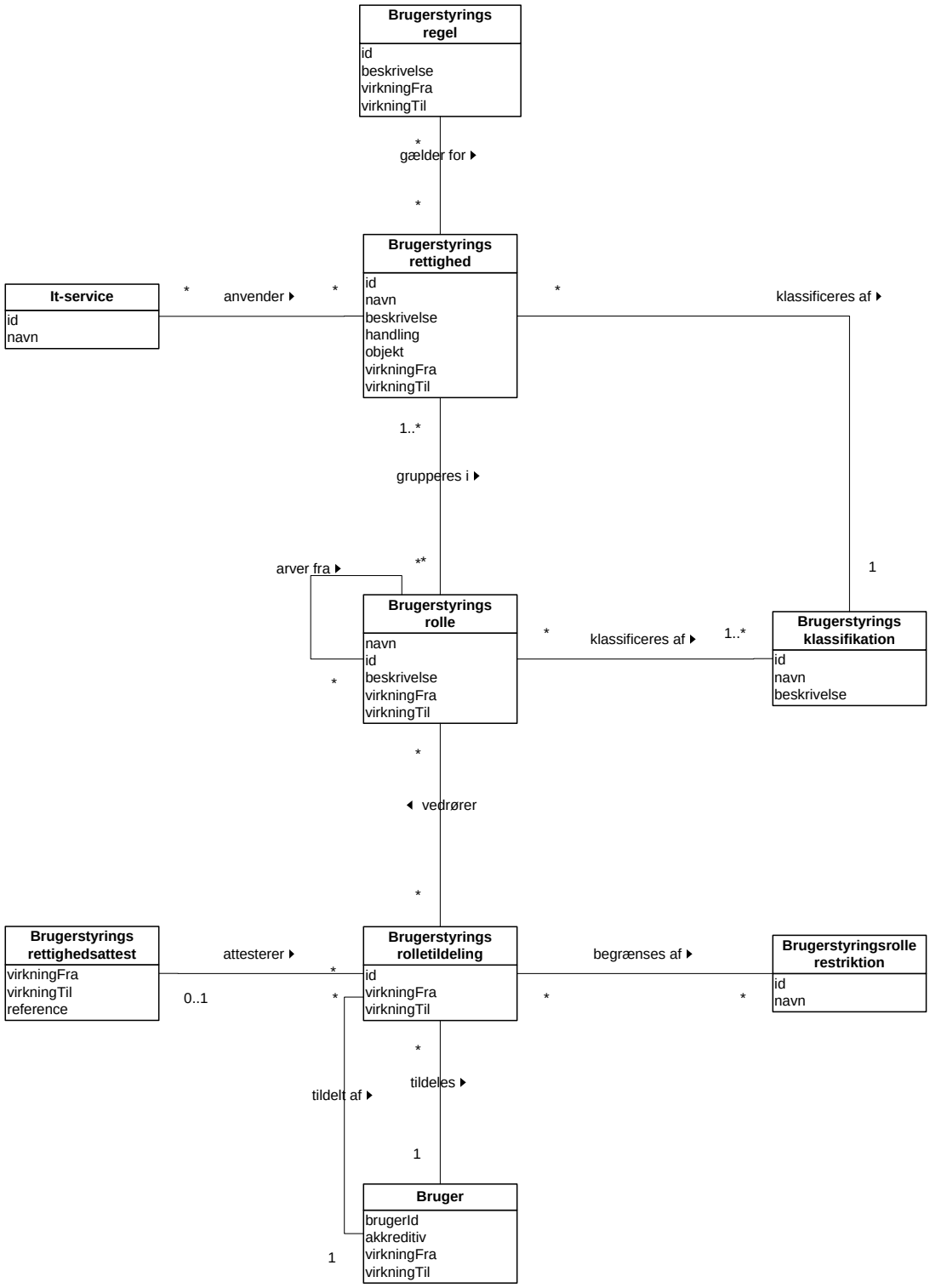
Den fællesoffentlige begrebsmodel for brugerstyring viser begreberne indenfor brugerstyring og deres indbyrdes relationer.

En bruger kan tildeles en række brugerstyringsroller, som kan begrænses i form af brugerstyringsrollerestriktioner. Tildelingen af brugerstyringsroller kan dokumenteres i form af en brugerstyringsrettighedsattest. En tildeling af brugerstyringsroller er altid foretaget af en anden bruger.

En bruger kan være enten en person eller et it-system. En person, eller for den sags skyld et it-system, kan optræde som mange brugere med hvert sit akkreditiv tilknyttet.

Brugerstyringsroller er grupperinger af brugerstyringsrettigheder. Brugerstyringsroller og brugerstyringsrettigheder kan klassificeres i henhold til brugerstyringsklassifikationer. Brugerstyringsrettigheder kan anvendes i forskellige it-services, og der kan være knyttet brugerstyringsregler til.

>


Brugerstyrings regel
id
beskrivelse
virkningFra
virkningTil
gælder for
Brugerstyrings rettighed
id
navn
beskrivelse
handling
objekt
virkningFra
virkningTil
It-service
id
navn
anvender
klassificeres af
grupperes i
arver fra
Brugerstyrings rolle
navn
id
beskrivelse
virkningFra
virkningTil
klassificeres af
Brugerstyrings klassifikation
id
navn
beskrivelse
vedrører
Brugerstyrings rettighedsattest
virkningFra
virkningTil
reference
attesterer
Brugerstyrings rolletildeling
id
virkningFra
virkningTil
begrænses af
Brugerstyringsrolle restriktion
id
navn
tildeles
tildelt af
Bruger
brugerId
akkreditiv
virkningFra
virkningTil

>

Begreber

Bruger

Definition:	En bruger er en person eller et it-system, der gør brug af services, som stilles til rådighed af et eller flere it-systemer.
Beskrivelse:	Bruger anvendes til at identificere en person eller et it-system med et akkreditiv (eksempelvis med et medarbejdercertifikat) og de rettigheder brugerstyringsaktøren har i forhold til en given service, der stilles til rådighed af et it-system.
Eksempler:	”170342-0618”, ”RIGET1747”
Informationsindhold:	• brugerId Identificerer brugeren overfor den service der anvendes. • akkreditiv Angiver det akkreditiv der autentificerer brugeren overfor servicen, fx digital signatur eller medarbejdercertifikat. • virkningFra Angiver datoen hvor brugeren er aktiv fra. • virkningTil Angiver den dato hvor brugeren deaktiveres.

Brugerstyringsrolle

Definition:	Beskriver den autoritet og det ansvar, som er givet til de brugere, som brugerstyringsrollen er tildelt.
Beskrivelse:	Brugerstyringsroller anvendes til at afgøre, hvilke handlinger en bruger må udføre i et it-system. Brugerstyringsrollen fastlægger de rettigheder, som brugeren er tildelt, men den har intet at gøre med formålet med at udføre disse handlinger. Brugere tilknyttes til roller og opnår rettigheder ved at være rolleindehaver. Brugerstyringsroller er grupperinger af rettigheder, og der er ikke nødvendigvis sammenfald mellem brugerstyringsroller og brugerens profession, stillingsbetegnelse mv.
Eksempler:	Læge, Sygeplejerske, SygeplejerskeOrd, Lønindberetter
Informationsindhold:	• id Unik identifikation af brugerstyringsrollen. • navn

>

Brugerstyringsrollens navn.

- beskrivelse
  En beskrivelse af rollen.

- virkningFra
  Angiver rollens ikrafttrædelsesdato.

- virkningTil
  Angiver den dato hvor rollen ophører.

Brugerstyringsrettighed

Definition: Beskriver en specifik rettighed til at foretage en handling på et objekt.

Beskrivelse: Brugerstyringsrettigheder anvendes til at afgøre om en bruger må udføre en specifik handling på et objekt.

Eksempler: OpretSag, Bogføring, PersonData

Informationsindhold:

- id
  Unik identifikation.

- navn
  Navnet på brugerstyringsrettigheden.

- beskrivelse
  En beskrivelse af brugerstyringsrettigheden.

- handling
  En beskrivelse af den tilladte handling.

- objekt
  En beskrivelse af det objekt som handlingen må foretages på.

- virkningFra
  Den dato hvor brugerstyringsrettigheden kan anvendes.

- virkningTil
  Den dato hvor brugerstyringsrettigheden ikke længere kan anvendes.

Brugerstyringsklassifikation

Definition: Beskriver forskellige klassifikationer i forhold til hvilke, brugerstyringsroller og brugerstyringsrettigheder kan klassificeres.

Beskrivelse: Brugerstyringsklassifikationer anvendes til at klassificere brugerstyringsroller og brugerstyringsrettigheder inden for

forskellige områder.

Brugerstyringsklassifikationen giver mulighed for, at de forskellige myndigheder, forvaltningsområder m.m. (eksempelvis Sundhed) kan anvende deres egne brugerstyringsroller og brugerstyringsrettigheder.

Eksempler: FORM, Sundhed, Fællesoffentlig

Informationsindhold:

- id
  Unik identifikation.
- navn
  Navnet på brugerstyringsklassifikationen.
- beskrivelse
  En beskrivelse af brugerstyringsklassifikationen.

Brugerstyringsrollerestriktion

Definition: Kan begrænse en brugerstyringsrolletildeling ift. en organisation, person mv.

Beskrivelse: En brugerstyringsrollerestriktion er en relevant aktør, fx person, organisation eller system - set i brugerstyringssammenhæng - som brugerstyringsrolletildelingen begrænses til.

Eksempler: Hans Hansen, Rigshospitalet, Århus Kommune, Økonomistyrelsen

Informationsindhold:

- id
  Unik identifikation.
- navn
  Brugerstyringsrestriktionens navn.

Brugerstyringsrolletildeling

Definition: Beskriver hvilke roller en bruger er tildelt i forhold til brugerstyringsrollerestriktioner.

Beskrivelse: Brugerstyringsrolletildelingen anvendes til at kunne begrænse gyldigheden af en brugers tildelte brugerstyringsroller i forhold til bestemte brugerstyringsrollerestriktioner.

Eksempler:

Informationsindhold:

- id
  Entydig identifikation af forekomster.
- virkningFra

>

Angiver ikrafttrædelsesdato.

- virkningTil
  Angiver ophørsdato.

Brugerstyringsrettighedsattest

Definition:	Beskriver den dokumentation der ligger til grund for tildelingen af brugerstyringsrollerne.
Beskrivelse:	Tildeling af roller kræver ofte en attestation, der dokumenterer gyldigheden af tildelingen. Dokumentationen kan fx være en fuldmagt, eller underskrift af nærmeste chef.
Eksempler:	Kontrakt, Fuldmagt
Informationsindhold:	• virkningFra Den dato hvorfra brugerstyringsrettighedsattesten er gyldig. • virkningTil Den dato hvor brugerstyringsrettighedsattesten ophører med at være gyldig. • reference Angiver en reference til de attester der ligger til grund for tildelingen

Brugerstyringsrettighedsudsteder

Definition:	Beskriver den person eller organisation der attesterer brugerstyringsrettighedstildelingen.
Beskrivelse:	Brugerstyringsrettighedsattester udstedes af enten en person eller en organisation. Brugerstyringsrettighedsudsteder anvendes til at identificere denne person eller organisation.
Eksempler:	Århus Kommune, Brugeradministrator, Security Token Service
Informationsindhold:	

Brugerstyringsregel

Definition:	Beskriver en brugerstyringsregel som er gældende for en eller flere brugerstyringsrettigheder.
Beskrivelse:	Brugerstyringsregler beskriver regler der er gældende for en eller flere brugerstyringsrettigheder. Regler kan være simple, fx ved at begrænse anvendelsen af en rettighed til et bestemt tidsrum, eller komplekse ved fx at udpege brugerstyringsregler der udelukker hinanden.

>

Eksempler:

Informationsindhold:

- id
  Entydig identifikation af brugerstyringsreglen.
- beskrivelse
  En beskrivelse af brugerstyringsreglen.
- virkningFra
  Den dato hvorfra brugerstyringsreglen er gyldig.
- virkningTil
  Den dato hvor brugerstyringsreeglen ophører med at være gyldig.

Relationer

Brugerstyringsrolletildeling *begrænses af* Brugerstyringsrollerestriktion

Definition: Begrænser de rettigheder som brugerstyringsrollerne giver brugeren til kun at gælde overfor den udpegede brugerstyringsrollerestriktion.

Beskrivelse: En bruger kan have tildelt mange brugerstyringsroller, men tildelingen af rollerne kan være begrænset i forhold til fx en specifik organisation eller person. Fx kan det tænkes at en sygeplejerske har ordinationsret på et sygehus, men ikke nødvendigvis på alle andre sygehuse.

Brugerstyringsrolletildelingen kan udpege flere brugerstyringsrollerestriktioner. Dvs. at en brugerstyringsrolletildeling begrænses til de udpegede brugerstyringsrollerestriktioner.

En brugerstyringsrollerestriktion kan begrænse mange brugerstyringsrolletildelinger.

Brugerstyringsrolletildeling *tildeles* Bruger

Definition: En brugerstyringsrolletildeling peger altid den bruger ud, som den givne kombination af brugerstyringsroller og brugerstyringsrollerestriktioner er gældende for.

Beskrivelse: Den samme brugerstyringsrolle kan tildeles mange brugere. Relationen anvendes til at udpege netop en specifik kombination af brugerstyringsroller og brugerstyringsrollerestriktioner i forhold til en given bruger.

En brugerstyringsrolletildeling udpeger altid en og kun en bruger.

>

En bruger kan have mange brugerstyringsrolletildelinger.

Brugerstyringsrolletildeling *vedrører* Brugerstyringsrolle

Definition: Udpeger de brugerstyringsroller som den givne kombination af bruger og brugerstyringsrollerestriktioner er tildelt.

Beskrivelse: Brugere kan have tildelt mange brugerstyringsroller. Relationen anvendes til at udpege hvilke brugerstyringsroller der er gældende for en specifik kombination af bruger og brugerstyringsrollerestriktioner.

En brugerstyringsrolletildeling vedrører en eller flere brugerstyringsroller.

En brugerstyringsrolle kan indgå i mange brugerstyringsrolletildelinger.

Brugerstyringsrettighedsattest *attesterer* Brugerstyringsrolletildeling

Definition: Hvis der foreligger en attestation af brugerstyringsrolletildelingen så udpeger relationen denne.

Beskrivelse: Somme tider kræver tildelingen af en brugerstyringsrolle dokumentation for retten til denne tildeling. Det kunne fx være et fuldmagtsdokument.

En brugerstyringsrettighedsattest kan attesterer mange brugerstyringsrolletildelinger.

En brugerstyringsrolletildeling kan være dokumenteret af en brugerstyringsrettighedsattest.

Brugerstyringsrolletildeling *tildelt af* Bruger

Definition: Udpeger den bruger der har foretaget brugerstyringsrolletildelingen.

Beskrivelse: En brugerstyringsrolletildeling er altid tildelt af en og kun en bruger.

En bruger kan have tildelt mange brugerstyringsrolletildelinger.

Brugerstyringsrettighed *grupperes i* Brugerstyringsrolle

Definition: Grupperer brugerstyringsrettigheder i brugerstyringsroller.

Beskrivelse: En brugerstyringsrettighed kan grupperes i flere brugerstyringsroller.

En brugerstyringsrolle kan indeholde flere brugerstyrings-

rettigheder.

Brugerstyringsrettighed *klassificeres af* Brugerstyringsklassifikation

Definition: Udpeger klassifikationen af en brugerstyringsrettighed.

Beskrivelse: En brugerstyringsrettighed klassificeres altid i forhold til en og kun en brugerstyringsklassifikation.

En brugerstyringsklassifikation kan klassificere brugerstyringsrettigheder.

Brugerstyringsrolle *klassificeres af* Brugerstyringsklassifikation

Definition: Udpeger klassifikationen af brugerstyringsrollen.

Beskrivelse: En brugerstyringsrolle er altid klassificeret i forhold til mindst en brugerstyringsklassifikation.

En brugerstyringsklassifikation kan klassificere brugerstyringsroller.

Brugerstyringsrolle *arver fra* Brugerstyringsrolle

Definition: En brugerstyringsrolle kan arve brugerstyringsrettigheder fra en anden brugerstyringsrolle.

Beskrivelse: For at lette administrationen af brugerstyringsroller, er det muligt at lade en brugerstyringsrolle arve brugerstyringsrettigheder fra andre brugerstyringsroller.

En brugerstyringsrolle kan arve brugerstyringsrettigheder fra flere brugerstyringsroller.

En brugerstyringsrolle kan nedarves til flere brugerstyringsroller.

Brugerstyringsrettighedsattest *udstedt af* Brugerstyringsrettighedsudsteder

Definition: Identificerer den brugerstyringsrettighedsudsteder der har udstedt brugerstyringsattesten.

Beskrivelse: En brugerstyringsrettighedsattest er altid udstedt af en og kun en brugerstyringsrettighedsudsteder.

En brugerstyringsrettighedsudsteder kan have udstedt flere brugerstyringsrettighedsattester.

Brugerstyringsregel *gælder for* Brugerstyringsrettighed

Definition: Udpeger hvilke brugerstyringsregler der er gældende for hvilke brugerstyringsrettigheder.

Beskrivelse: Der kan være forskellige regler gældende for forskellige brugerstyringsrettigheder.

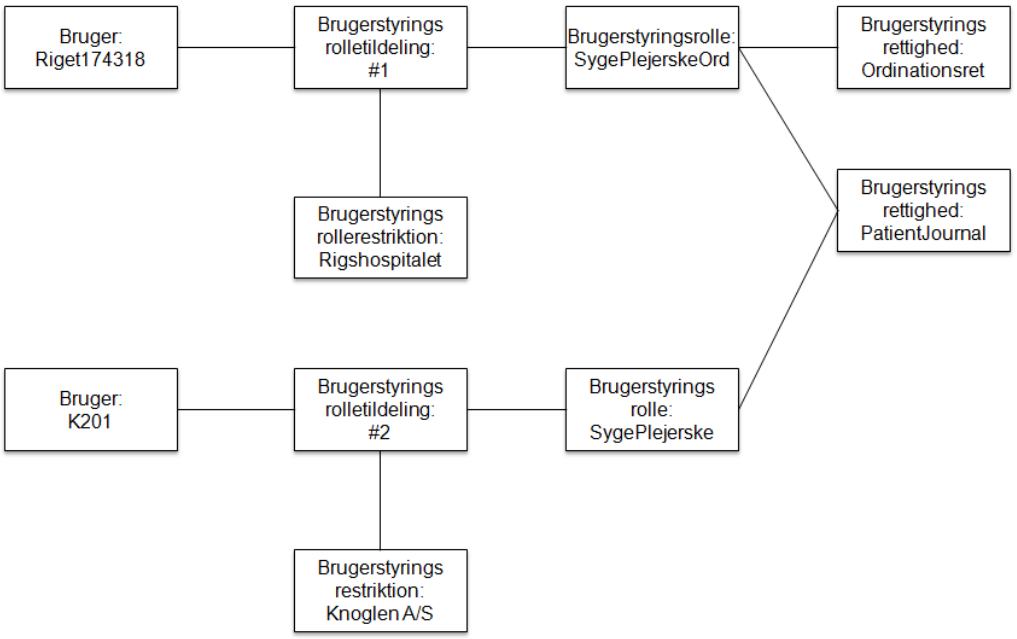
>

En brugerstyringsregel kan være gældende for flere brugerstyringsrettigheder.

En brugerstyringsrettighed kan have tilknyttet flere brugerstyringsregler.

Modeleksempler

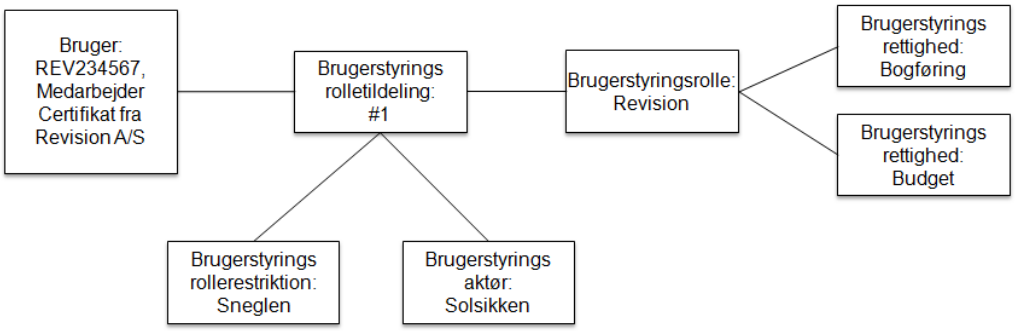
Scenarie 1: Sygeplejerske med to ansættelsesforhold
Nedenstående eksempel illustrerer et eksempel hvor en person har to ansættelsesforhold. I den forbindelse er der oprettet to brugere; begge brugere er knyttet til den samme person (fremgår ikke af eksemplet) nemlig den person der har de to ansættelsesforhold.
Den ene bruger er oprettet i forbindelse med personens ansættelsesforhold på Rigshospitalet, hvor brugeren har fået tildelt brugerstyringsrollen ”SygeplejerskeOrd”. Brugerstyringsrollen ”SygeplejerskeOrd indeholder to brugerstyringsrettigheder: ”Ordinationsret” og ”Patientjournal”.
Den anden bruger anvender personen i forhold til sit andet ansættelsesforhold på privathospitalet ”Knoglen A/S”. På Knoglen A/S er brugeren tildelt rollen ”Sygeplejerske”. Brugerstyringsrollen ”Sygeplejerske” er kun tildelt brugerstyringsrettigheden ”Patientjournal”.



>

Scenarie 2: Revisor for

Nedenstående eksempel viser en bruger, der er ansat i revisionsfirmaet Revision A/S. Der er oprettet en bruger med medarbejdercertifikat fra Revision A/S. Firmaet udfører revision for en række institutioner og brugeren er derfor tildelt brugerstyringsrollen Revision. Tildelingen af rollen er dog begrænset til to institutioner, hhv. Sneglen og Solsikken.

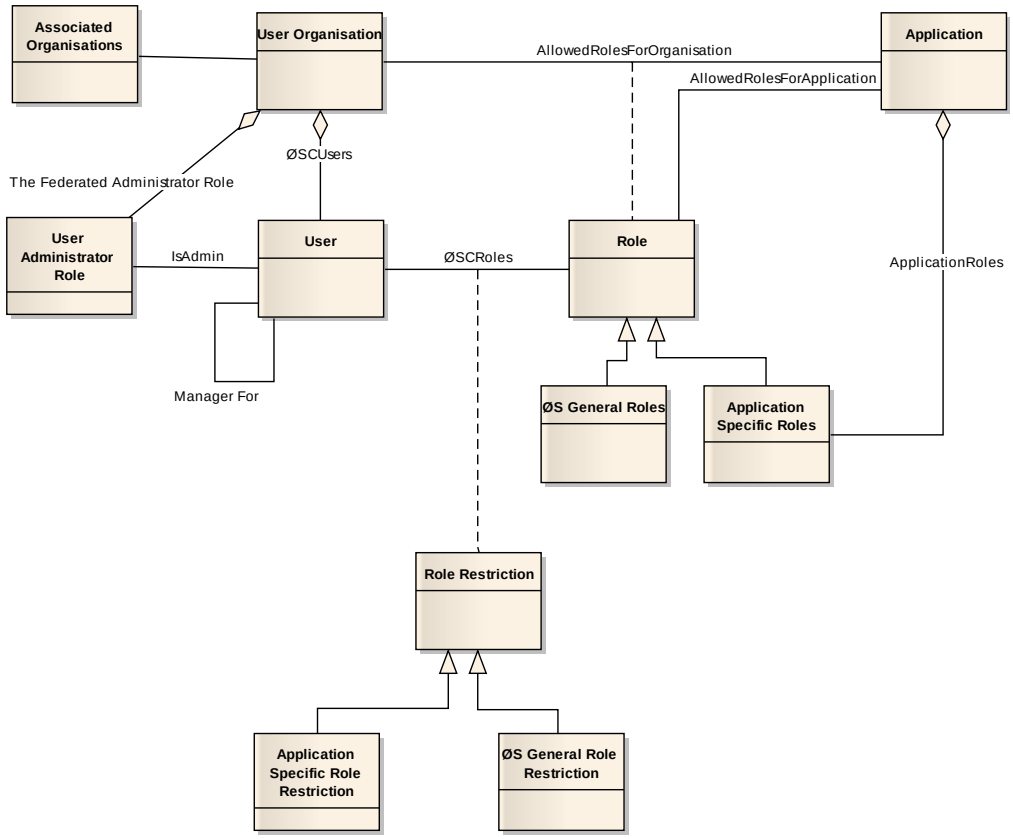


Del D – Anvendelsesscenarier

>

Økonomistyrelsen – BRL projektet

Økonomistyrelsen har et igangværende ”BRL projekt” omkring en brugerrettigheds løsning ril et blanketsystem, der anvendes til opgavebestilling fra ØSC’ets kunder til ØSC. I projektet er der udarbejdet nedenstående begrebsmodel - specifikt rettet mod det offentliges økonomiområde:



Modellen matcher på de fleste områder den fællesoffentlige begrebsmodel. Forskelle kan primært begrundes i det forhold, at BRL-modellen i den nuværende form har et mere begrænset scope.

Den grundlæggende modellering omkring bruger, rolle og rollerestriktion er samme struktur. Den fællesoffentlige model har mulighed for en bredere definition i forhold til rollerestriktioner, og der kan også knyttes et ”brugerstyringsattest” til den konkrete rolletildeling.

BRL-modellen opererer kun med roller og ikke med rettigheder. Dette er ikke noget problem, idet roller konceptuelt blot er en gruppering af nogle rettigheder.

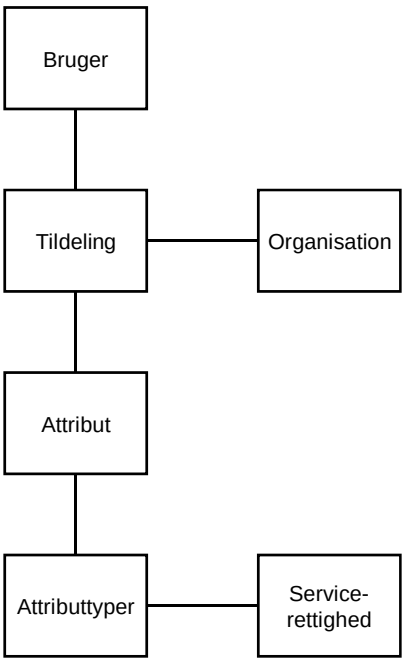
Tildeling af roller knytter BRL-modellen op mod organisation, hvilket er naturligt inden for det givne scope. I den fællesoffentlige begrebsmodel er der ikke denne binding, idet denne model også skal kunne rumme eksempelvis borgere med et OCES-certifikat.

>

I den fællesoffentlig begrebsmodel registreres den bruger, som har foretaget en konkret tildeling af en rolle til en bruger. I BRL-modellen registreres ikke på de enkelte tildelinger, men derimod blot på hvem der administrerer hvilke brugere.

Digital Sundhed

Digital Sundhed arbejder med modeller til implementering af brugerrettigheds løsninger, men p.t. er der ikke en egentlig begrebsmodel. Der arbejdes med nedenstående skitse til en begrebsmodel inden for digital sundhed:



Modellen er som nævnt ikke modelleret færdig p.t., men selve grundstrukturerne er meget sammenfaldende med den fællesoffentlige brugerstyringsmodel. Hos Sundhed er der p.t. anvendt begreber, som meget er fokuseret på, at implementeringen er tænkt gennemført vha. en attributserver.

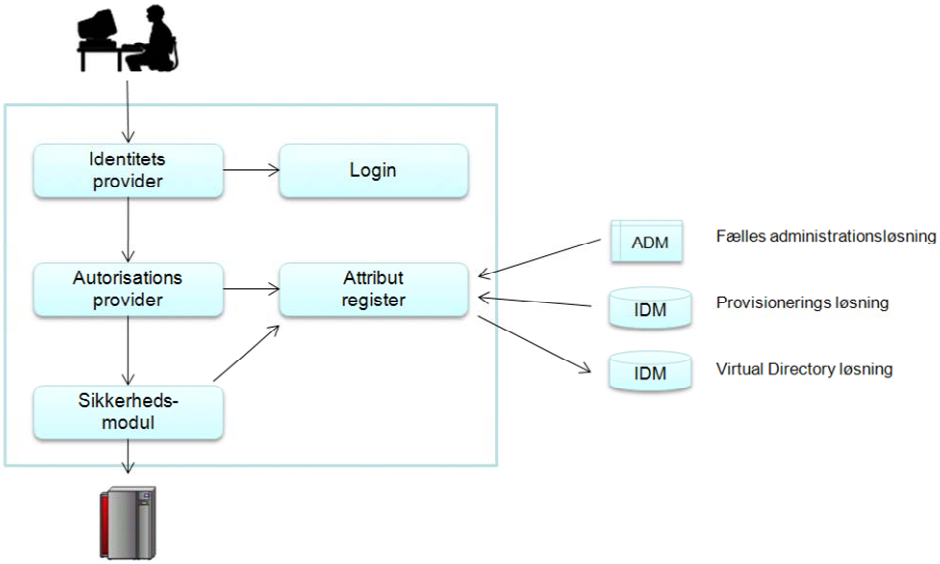
”Attribut” svarer stort set til det, der i den fællesoffentlige begrebsmodel kaldes for ”Brugerstyringsrolle”. Et eksempel på en ”Attribut” er ”Læge”. ”Attributtyper” svarer til en profil/jobfunktion og ”Servicerettighed” til en ”Brugerstyringsrettighed”. Der er omkring attribut, attributtype og servicerettighed stort set tale om en modellering af det, som i den fællesoffentlige brugerstyringsmodel kaldes for brugerstyringsrolle og brugerstyringsrettighed – blot modelleret med en lidt større granularitet.

Selve tildelingen af en rolle til en bruger er stærkt knyttet til ”Organisation”. Dette skyldes det forhold inden for Sundhed, at personer ofte har flere stillinger i forskellige organisationsenheder med forskellige rettigheder.
Denne modellering i forhold til organisation er i den fællesoffentlige begrebsmodel modelleret ved, at der til en given rolletildeling kan knyttes en rollerestriktion med angivelse af, at rollen kun kan udføres inden for den pågældende restriktion.

>

Anvendelse af et attributregister

I forbindelse med brugerrettighedsløsninger arbejder flere parter med en arkitektur baseret på et attributregister, eksempelvis som beskrevet i ” FBRS system analyse rapport version 1.0” dateret 22. Juni 2009. Heri er nedenstående principskitse præsenteret:



Figuren illustrerer et scenarie, hvor en bruger ønsker at tilgå en service. Først skal brugeren autentificeres. Derefter tilknyttes sessionen de gældende autorisationer. Brugerrettighedsløsningen tænkes her at spille rollen som attributregister, og således indirekte være styrende for, hvilke rettigheder brugeren opnår i den pågældende session. Attributterne kan være f.eks. roller/jobfunktioner kvalificeret med en angivelse af det organisatoriske niveau.

Den fysiske realisering af en attributservice arkitektur kan have mange varianter, men konceptuelt matcher modelleringen omkring den fællesoffentlige begrebsmodel fint disse tanker. Modelleringen indeholder en relation mellem it-service og brugerstyrings rettigheder, som fortæller, hvilke rettigheder der anvendes i den enkelte it-service. I en konkret arkitektur med en attributserver skal dette detaljeres ned til at kunne angive helt eksakt, hvilke attributter it-servicen har brug for, for at kunne verificere om de nødvendige rettigheder er til stede.

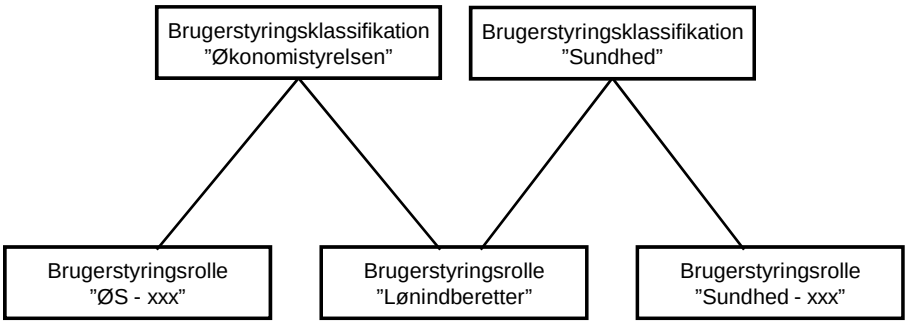
Mapning mellem roller

Brugerstyringsroller klassificeres af en eller flere brugerstyringsklassifikationer, dvs. at en brugerstyringsrolle kan være klassificeret som ”Fællesoffentlig”, ”Sundhed” etc. eller den kan være klassificeret som hørende til en konkret it-service/it-system.

Denne klassifikation gør det muligt at have egne brugerstyringsroller, men det giver også mulighed for at dele roller med andre.

Hvis vi eksempelvis antager, at der under klassifikationen ”Økonomistyrelsen” er defineret en rolle ”lønindberetter”, kan denne rolle – efter aftale med en anden myndig-

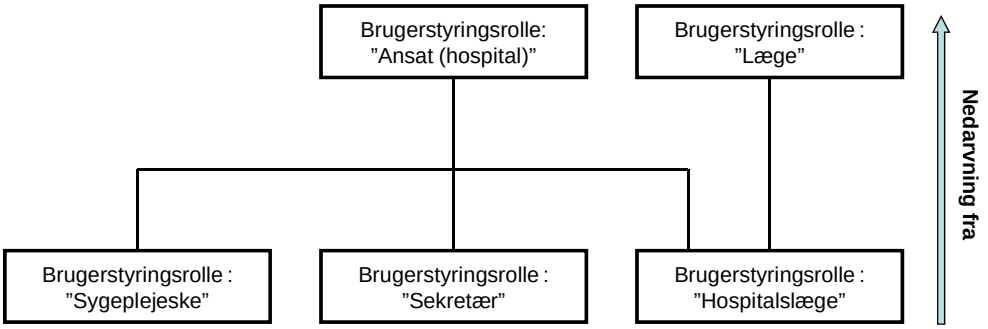
hed – deles med andre klassifikationer. Eksempelvis kan der være lavet en aftale med ”Sundhed” om at rollen ”lønindberetter” må anvendes inden for denne brugerstyrings-klassifikation.
Rollen ”lønindberetter” optræder herefter i to brugerstyringsklassifikationer:



”Sundhed” laver en mapning mod egen organisation og tildeler rollen til de personer i organisationen, som må foretage lønindberetning med de juridiske og økonomiske konsekvenser dette måtte have.

Nedarvning af roller

Begrebsmodellen er modelleret med mulighed for nedarvning af rettigheder fra andre roller, jf. nedenstående eksempel fra sundhedsvæsenet:



Såfremt en konkret implementering af modellen ikke kan håndtere denne form for nedarvning, vil den samme effekt kunne opnås ved at tilpasse den brugerflade, der administrere tildeling af roller, til at kunne håndtere nedarvning, selvom den underliggende datamodel kræver at rettighederne er knyttet direkte til rollen.