#

#

***Udvalget for Arkitektur og Standarder***

***Modelreview-rapport for begrebsmodellen:*
bruger- og adgangsstyring**

*til Referencearkitektur for brugerstyring v.1.1*

**Indhold**

[**Modelreview af begrebsmodellen for Bruger- og adgangsstyring**](#_w8n48xajgw0n) **2**

[**Generelle bemærkninger**](#_2et92p0) **3**

[**Vurderinger og anbefalinger**](#_n60evx6lmd0d) **3**

[**Anbefalinger til det nuværende projekt**](#_2kvt2tsi5f5f) **3**

[**Anbefalinger til det fremtidige arbejde**](#_9w2rdtg6chg6) **3**

[**Tværgående anbefalinger**](#_g090aukoxite) **4**

[**Regelgennemgang**](#_esxjn2786mjv) **4**

[**Bilag**](#_yebxrxcqvnpz) **10**

#

# Modelreview af begrebsmodellen for Bruger- og adgangsstyring

Denne rapport dokumenterer i hvilket omfang den indleverede model er i overensstemmelse med Fællesoffentlige regler for begrebs- og datamodellering (Modelreglerne).

Som grundlag for gennemgangen er anvendt version 2.0.0 af Modelreglerne.
<https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/modelregler>

Modelreviewet blev gennemført d. 14. april - 24. april 2020.

**Kort beskrivelse af modellen:**

Begrebsmodellen for bruger- og adgangsstyring er en kernemodel og indeholder relevante begreber for styring af brugere og deres adgang til forretningstjenester og de tillidstjenester der muliggøre dette. Den er udarbejdet i forbindelse med Fællesoffentlig Referencearkitektur for brugerstyring version 1.1.

**Afleveringen**
Modellen blev indleveret til modelreview d. 2.april 2020, og består af:

* Afleveringsdokumentation: Afleveringsdokumentation.docx
* Den fulde UML-model i xmi: brugeradgangsstyring\_0.9.0.xml
* Begrebsliste i Excel: brugeradgangstyring\_0.9.0.xslx
* UML-diagrammer i billedformat:
	+ Oversigtsdiagram - Brugerstyring.png
	+ Kontekstdiagram - Adgang.png
	+ Kontekstdiagram - Adgangsbilletter og attributter.png
	+ Kontekstdiagram - Bruger og entitet.png
	+ Kontekstdiagram - Digital identitet og autentifikation.png
	+ Kontekstdiagram - Tjenestetyper.png

Derover henvises til modellens midlertidige webudstilllinger:

* UML-model: <http://data.gov.dk/test/udkast/Brugerstyring/UML>
* xmi : <https://data.gov.dk/test/udkast/Brugerstyring/brugeradgangstyring_0.9.0.xml>
* xlsx:: <https://data.gov.dk/test/udkast/Brugerstyring/brugeradgangstyring_0.9.0.xlsx>

**Reviewboard og deltagere**

|  |  |
| --- | --- |
| Reviewboard | Camilla Wiberg Danielsen, Sundhedsdatastyrelsen (primært ift. Regel 21) |
| Kim Newton Kassebeer, Styrelsen for Dataforsyning og Effektivisering  |
| Sekretariat for 8.1 | Anna Odgaard Ingram, Digitaliseringsstyrelsen  |
| Asbjørn Lauwersen, Digitaliseringsstyrelsen  |

# Generelle bemærkninger

Begrebsmodellen for ‘bruger- og adgangsstyring’ fremstår generelt gennemarbejdet og veldokumenteret med gode definitioner, udførlige modelmetadata og kildeangivelser.

# Vurderinger og anbefalinger

Her gives en oversigt over vurderinger og anbefalinger til det nuværende projekt og det fremtidige projekt samt anbefalinger af tværgående karakter.

**Beskrivelse af de forskellige typer af anbefalinger**

* Anbefalinger til det nuværende projekt: Herunder fremstår anbefalinger til projektet i dets nuværende og kommende faser, som det er præsenteret for reviewboardet.
* Anbefalinger til det fremtidige arbejde i forlængelse af projektet: Her indgår anbefalinger til fremtidigt opfølgende arbejde efter idriftsættelse.
* Tværgående anbefalinger: Disse anbefalinger identificeres af reviewboardet som centrale og relevante for projektets fremtidige succes, men samtidig af en sådan karakter, at disse udfordringer ikke kan løses af projektet isoleret set.

## Anbefalinger til det nuværende projekt

**1. Det anbefales, at det den engelske oversættelse af “*brugerstyring/bruger- og adgangsstyrin*g” genovervejes (*user management* vs. *identity (and access) managemen*t) og at projektet vurderer i hvilken grad der skal sikres overensstemmelse med og reference til centrale ‘Identity Management’ begreber fra ISO-standarderne ISO/IEC 29146:2016 - ‘I*nformation technology — Security techniques — A framework for access management*’, og ISO/IEC 24760: ‘*IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*’.**

**2. Det anbefales, at alene modelelementer som *tilhører* modellen forsynes med identifikatorer der tager udgangspunkt i modellens namespace.**

**3. Det anbefales, at projektet behandler de væsentligste kommentarer til definitionerne under Regel 21, og forholder sig til de øvrige mindre sproglige ændringsforslag i bilag.**

## Anbefalinger til det fremtidige arbejde

**4. Det anbefales, at det ved en eventuel fremtidig revision undersøges om der er internationale specifikationer under udvikling eller opdatering for ‘Identity and Access Management’ fra eksempelvis W3C eller ISO. Der forventes at W3C vil etablere modeller for dette emneområde. Der pågår eksempelvis et W3C-arbejde omkring “decentralized identity management” som kunne blive relevant. Eventuelle opdateringer af førnævnte ISO-standarder ISO/IEC 29146:2016 og ISO/IEC 24760 bør også undersøges.**

## Tværgående anbefalinger

**5. Det anbefales, at det i vejledningen til modelreglerne fremgår tydeligt at begrebsmodeller også forsynes med identifikatorer, og at denne oplysning tydeligt fremgår i skabelonen til registrering af begreber i regneark.**

**6. Det anbefales, at kommentarer/ændringsforslag til begreber som ikke defineres men genbruges af denne begrebsmodel i det omfang det er muligt kommunikeres tilbage til de modelansvarlige parter.**

# Regelgennemgang

**Overholdt**:
GRØN=Regel overholdt,
GUL= Regel delvist overholdt
RØD= Regel ikke overholdt,
HVID=BØR/KAN-regel (Dvs: ikke krav eller hvis den angivne elementtype ikke indgår i modellen)

Se oversigt over modelregler 2.0 her: <https://arkitektur.digst.dk/modelregler2---liste>

##

**Generelt:**

**01** - [**Brug UML som det visuelle modelsprog**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/brug-uml-som-det-visuelle-modelsprog)Reglen er fulgt

**02 -** [**Brug kun udvalgte UML-elementer**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/brug-kun-udvalgte-uml-elementer)Reglen er fulgt

**03 -** [**Brug UML-stereotyper**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/brug-uml-stereotyper)Reglen er fulgt. Alle begreber har stereotypen <<Concept>> og selve begrebsmodellen har stereotypen <<ConceptModel>>. Derudover er modellen klassificeret som en kernemodel (core model) via tagget modelScope.

**04 -** [**Udstil modellen online**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/udstil-modellen-online)Reglen er fulgt. Modellen er i forbindelse med modelreviewet blevet udstillet online på en midlertidig webadresse, <https://data.gov.dk/test/udkast/Brugerstyring/UML/>

Det er derudover planlagt at modellen udstilles endeligt ved godkendelse i Udvalget for Arkitektur og Standarder Q3 2020..

**05 -** [**Gør modellen tilgængelig i maskinlæsbart format**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/goer-modellen-tilgaengelig-i-maskinlaesbart-format)Reglen er fulgt. Modellen er afleveret i XMI-format og som regneark.

**Modeller**

**06 -** [**Angiv meningsfyldte navne og beskrivelser for modeller**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-meningsfyldte-navne-og-beskrivelser-modeller)
Reglen er fulgt. Modellen har fået navnet “Bruger-og adgangsstyring” i regnearket og UML-pakken har samme værdi i tagget label (da). Dette navn svarer til modellens indhold af begreber.

Selve UML-pakken har dog navnet “Referencearkitektur for brugerstyring, v 1.1”. Navnet bør svare til indholdet i label (da). Det bemærkes også at der således er en mindre overensstemmelse mellem referencearkitekturens titel og begrebsmodellen.

Hvis de begge antages at dække samme emneområde og ‘brugerstyring’ vurderes at rumme ‘adgangsstyring’, så kunne modellen evt alene benævnes ‘brugerstyring’? Fra referencearkitekturen har vi også at “*Aktiviteterne, der indgår i brugerstyring, kan overordnet opdeles i administration* (red: af digitale identiteter) *og adgangskontrol*.” Ellers kunne en opsplitning i to modeller (hhv. brugerstyring og adgangsstyring) evt. være relevant?

**07 -** [**Angiv identifikation af modeller**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-identifikation-af-modeller)
Reglen er fulgt. UML-pakken er forsynet med værdien [https://data.gov.dk/model/concept/brugeradgangsstyring#](https://data.gov.dk/model/concept/brugeradgangsstyring) i tagget namespace.

URIen følger de aktuelle retningslinjer for stabile URIer, men det forventes at begrebsmodeller ved en kommende revision anbefales placeret under ‘concept’ i stedet for ‘model’, at begrebsmodeller også inddeles i ‘core’ og ‘profile’ og at skilletegnet ‘#’ erstattes med ‘/’. Derudover er modellen blevet oversat til engelsk, så det bør overvejes om fragmentnavnet kunne tage afsæt i den engelske oversættelse for at understøtte bedre international sammenhæng.

I forhold til den engelske oversættelse af “*brugerstyring*” og “b*ruger- og adgangstyring*”, så bør det undersøges om termerne “i*dentity management (forkortet IdM)*” som bruges synonymt med “identity and access management (akronym IAM evt. også IdAM)” kunne være at foretrække fremfor “user management”.
(Se evt. <https://www.iso.org/standard/77582.html> og <https://en.wikipedia.org/wiki/Identity_management>)

Forslag til ny URI: [https://data.gov.dk/concept/core/identity-management/](https://data.gov.dk/concept/core/user-and-access-management/)

Den endelige namespace-værdi bør også indsættes i regnearket.
(hvor denne række pt. er skjult) inden endelig udstilling).

**08 -** [**Angiv den modelansvarlige organisation**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-den-modelansvarlige-organisation)Reglen er fulgt. Digitaliseringsstyrelsen er angivet som den modelansvarlige organisation.

**09 -** [**Angiv emneområde for modellen**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-emneomraade-modellen)Reglen er fulgt. 06.38.10.20 Tværgående it-løsninger til den digitale infrastruktur (FORM) er angivet.

**10 -** [**Angiv modellens version**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-modellens-version)Reglen er fulgt. Versionsnummeret et angivet som 0.9.0.

Seneste ændringsdato er angivet som 01-04-2020.
Datoen bør dog opbygges iht. xsd:dateTime (YYYY-MM-DD), hvilket ikke umiddelbart kan overholdes i Sparx EA.

**11 -** [**Modellen skal forretningsgodkendes**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/modellen-skal-forretningsgodkendes)Reglen er fulgt. Modellen planlægges godkendt i Udvalget for Arkitektur og Standarder (UAS) Q3 2020.

**12 -** [**Angiv modellens modelstatus**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-modellens-modelstatus)Reglen er fulgt. Modelstatus er angivet som ‘development’ (under udvikling)

**13 -** [**Angiv modellens lovgrundlag**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-modellens-lovgrundlag)Reglen er fulgt. Der er angivet både lovgrundlag og anden kilde.

* <http://data.europa.eu/eli/reg/2014/910/oj>
* <http://www.retsinformation.dk/eli/lta/2016/617>
* <https://digst.dk/media/20287/national-standard-for-identiteters-sikringsniveauer-nsis-version-201.pdf>

Projektet bør dog i forhold til øvrige kilder vurdere i hvilken grad der skal sikres overensstemmelse med eller genbrug af centrale ‘Identity Management’-begreber fra ISO-standarderne [ISO/IEC 29146:2016 - ‘Information technology — Security techniques — A framework for access management](https://www.iso.org/standard/45169.html)’, eller [ISO/IEC 24760: ‘IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts’.](https://www.iso.org/standard/77582.html)

**14 -** [**Etablér sammenhæng mellem begrebsmodeller og logiske modeller**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/etabler-sammenhaeng-mellem-begrebsmodeller-og-logiske)Ikke relevant

**15 -** [**Modeller klassifikationer til genbrug**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/modeller-klassifikationer-til-genbrug)Ikke relevant

**Modelelementer**

**16 -** [**Angiv meningsfyldte UML-navne for modelelementer**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-meningsfyldte-uml-navne-modelelementer)
Reglen er fulgt.

Det bemærkes at der er anvendt flere engelske termer, men antages at dette er udtryk for at der ikke findes danske termer for disse begreber. fx ‘*verified claim’, ‘self-asserted claim’, ‘bootstrap token’,* og de dansk-engelsk-sammensatte termer *‘attended softwarerobot’ og ‘discovery-tjeneste’.*

**17 -** [**Giv alle modelelementer en identifikator**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/giv-alle-modelelementer-en-identifikator)Reglen er delvist fulgt.

Alle begreber i UML-modellen blevet forsynet med identifikatorer, men identifikatorer dannes alene i forbindelse med modellering af *kernemodeller* ved at danne en fuldt kvalificeret HTTP-URI som en sammensætning af det namespace der identificerer den model elementet tilhører samt et fragmentnavn som placeres efter skilletegnet.

Alene de begreber der tilhører kernemodellen ‘bruger- og adgangsstyring’ skal have identifikatorer med dettes namespace.

(Der anføres en tværgående anbefaling pga. denne problemstilling)

**18 -** [**Angiv termer i et naturligt sprog**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-termer-i-et-naturligt-sprog)Reglen er fulgt. Der er registreret både foretrukne termer, accepterede termer samt enkelte frarådede termer i et naturligt sprog.

For termen *‘brugerstyring’* kunne man overveje at tilføje *‘identitetsstyring’* som accepteret synonym term.

**19 -** [**Brug standardiserede konventioner for angivelse af navne**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/brug-standardiserede-konventioner-angivelse-af-navne)Reglen er fulgt. Termer og relationer er angivet med lille begyndelsesbogstav, efter gældende retstavning og mellemrum er anvendt til adskillelse af ord.

Obs. I definitionen af ‘digital identitet’ anvendes dog forkortelsen ‘v.hj.a’. Retskrivningsordbogen angiver ‘vha.’ (el. ved hj. af) som forkortelse for ‘ved hjælp af’

Obs: I ordlisten til referencearkitekturen (som dog ikke er genstand for dette review) har termer en blanding af store og små bogstaver.

**20 -** [**Udarbejd definitioner eller beskrivelser af modellens elementer**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/udarbejd-definitioner-eller-beskrivelser-af-modellens)

Reglen er fulgt. Alle begreber er forsynet med definitioner.

**21 -** [**Udarbejd strukturerede definitioner på en standardiseret måde**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/udarbejd-strukturerede-definitioner-paa-en-standardiseret)Reglen er fulgt i al væsentlighed. Definitionerne er opbygget som indholdsdefinitioner, hvor nærmeste overbegreb nævnes efterfulgt af adskillende træk.

Her følger væsentlige kommentarer til definitionerne
(se også [bilag](https://docs.google.com/document/d/1Q9Hm9SVGsMI-2UJALclWhv-H9DKVWy2IR-lW6OHfmII/edit?usp=sharing) med mindre sproglige ændringsforlag):

**autentifikationsfaktor:**

Definitionen af autentifikationsfaktor indledes med stort begyndelsesbogstav, som bør ændres til lille begyndelsesbogstav inden udstilling, og samme definition indeholder også hvad der eventuelt kan betragtes som supplerende noter der med fordel kan anføres i en kommentar:

autentifikationsfaktor (forslag):

Definition: egenskab ved et identifikationsmiddel, der binder det til entiteten

Kommentar: En autentifikationsfaktor kan kategoriseres som:
a) indehaverbaseret autentifikationsfaktor: en autentifikationsfaktor, som entiteten skal bevise at være i besiddelse af (fx en fysisk enhed)
b) vidensbaseret autentifikationsfaktor: en autentifikationsfaktor, som Entiteten skal bevise at have kendskab til (fx et kodeord)
c) iboende autentifikationsfaktor’: en autentifikationsfaktor, der er baseret på et fysisk træk hos en fysisk person, og som entiteten skal bevise at have (fx biometri)

**attribut:**

Definitionen lyder “e*genskaber der kan knyttes til en digital identitet*” (flertal). Vil én attribut svare til mere end én egenskab, eller vil “*egenskab der kan knyttes til en digital identitet*” (ental) være at foretrække?

 **entitet**

I FORVIR og NBS Begrebsbasen er det fx det allerøverste topbegreb, og er derfor overbegreb for både begrebet aktivitet og begrebet objekt. En type objekt er begrebet aktør - det vil måske være mere korrekt at anvende ‘objekt’ her. En aktør kan her være en organisation, et system eller en person.

**delegering**

Sædvanligvis følger der ansvar med delegering - dette kunne med fordel indgå i definitionen.

**fuldmagt**
Der mangler en væsentlig detalje i definitionen nemlig, at det er noget man giver.

**organisation**

Denne definition er følger ikke anbefalingerne omkring definitioner.

Definitionen af organisation indeholder ordet ‘især’ som indikerer at dette ikke altid gælder, hvorfor dette ikke bør indgå i definitionen, men da dette er en oversættelse af W3Cs definition af organisaiton i Organisationsontologien vejer dette genbrugshensyn tungere end definitionsopbygningen.

organisation:

Definition: en organisation, der –især i juridisk forstand –er bredt anerkendt og har tilhørende rettigheder og ansvar

Oprindelig definition “An Organization which is recognized in the world at large, in particular in legal jurisdictions, with associated rights and responsibilities”

*Generelt:*

For langt størstedelen af definitionerne sættes der ikke komma efter ‘der’ og ‘som’.
Der er ganske definitioner hvor man derfor evt. kunne fjerne kommaet:
fx (adgangskontrol): “proces, der..”

**22 -** [**Udarbejd anvendelsesneutrale definitioner**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/udarbejd-anvendelsesneutrale-definitioner)Reglen er fulgt.

**23 -** [**Angiv modelelementers lovgrundlag**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-modelelementers-lovgrundlag)Reglen er fulgt. Der er angivet både lovgrundlag og øvrige kilder.

**24 -** [**Definér kun nye modelelementer når det er nødvendigt**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/definer-kun-nye-modelelementer-naar-det-er-noedvendigt)Reglen er fulgt.

Der er genbrugt modelelementer fra flere eksterne kilder, men det bør undersøges nærmere som der eksisterer ISO-begreber som med fordel kunne genbruges. Se også kommentar vedr. regel 13.

**25 -** [**Sammensæt anvendelsesmodeller af elementer fra kernemodeller**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/sammensaet-anvendelsesmodeller-af-elementer-fra)Reglen er ikke relevant for kernemodeller.

**26 -** [**Angiv om begrebet tilhører modellens emneområde**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/angiv-om-begrebet-tilhoerer-modellens-emneomraade)Reglen er fulgt. Begreberne i regnearket er forsynet med en ja/nej-markering og de genbrugte begreber i UML-modellen har fået en (blå) farvemarkering.

Det bemærkes dog at kolonneoverskriften til markering af om begrebet tilhører modellens emneomrøde ikke bør være ‘eget’ men ‘tilhører emneområde’
(Kolonneoverskriften ‘eget’ stammer fra en tidligere skabelon til v.1 af Modelreglerne)

**27 -** [**Brug standardiserede primitive datatyper**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/brug-standardiserede-primitive-datatyper)Ikke relevant

**28 -** [**Modellér klassifikationsemner som instanser**](https://arkitektur.digst.dk/metoder/regler-begrebs-og-datamodellering/modeller-klassifikationsemner-som-instanser)Ikke relevant

# Bilag

Se mindre sproglige ændringsforslag og kommentarer til begreberne fra Camilla Wiberg Danielsen (SDST) på dette link: <https://docs.google.com/document/d/1Q9Hm9SVGsMI-2UJALclWhv-H9DKVWy2IR-lW6OHfmII/edit?usp=sharing>