Fællesoffentlig referencearkitektur for deling af data og dokumenter

Oktober 2017

Version 0.1, september 2017. Arbejdsdokument, der bygger oven på en tidligere udarbejdet Synopsis for Referencearkitektur for deling af data og dokumenter, august 2017. Benyttet i workshop med arkitektarbejdsgruppen under SDA.

Version 0.2, primo oktober 2017. Arbejdsdokument benyttet i forbindelse med anden workshop med arkitektarbejdsgruppen under SDA.

Version 0.3, medio oktober 2017. Opdateret med input fra anden workshop. Udgør Delleverance 2 ift. projektet Referencearkitektur for deling af data og dokumenter.

Resume

Hverdagen er digital, og data om borgere, virksomheder, myndigheder, ejendomme, steder, køretøjer o.m.m. vedligeholdes i en lang række områder af den offentlige administration. Der ligger et stort potentiale i at gøre sådanne data tilgængelige for genbrug, så de kan skabe værdi i andre sammenhænge end formålet med det oprindelige register. Dette kan danne fundament for langt bedre understøttelse af tværgående, offentlige services, og åbner tillige for anvendelse af data i nye og innovative sammenhænge.

Men deling af data kan være teknisk kompliceret og i mange tilfælde omkostningstungt, bl.a. drevet af krav til sikkerhed og dermed bevarelse af borgeres og virksomheders tillid til datadeling i det offentlige Danmark. Derfor er potentialet i deling og genbrug af data i høj grad forblevet uindfriet.

Denne referencearkitekturs formål er at hjælpe med at indfri dette potentiale. Dette gøres ved at introducere en fælles beskrivelse af de begreber og sammenhænge, der er væsentlige for at forstå og arbejde med design og implementering af løsninger, der involverer deling af data og dokumenter. Dette sker både på det strategiske plan, hvor vision, mål og arkitektoniske principper fastlægges; på det forretningsmæssige plan, hvor de typiske brugsscenarier beskrives; og på det tekniske plan, hvor en række implementeringsmønstre angiver, hvordan man i og mellem applikationer kan dele og forsende data.

Referencearkitekturen er udarbejdet under den fællesoffentlige digitaliseringsstrategi 2016-2020 og er som sådan relevant for alle offentlige myndigheder og deres leverandører samt for virksomheder, der ønsker at gøre brug af offentlige data.

1 Introduktion

1.1 Formål og målgruppe

Referencearkitekturen for deling af data og dokumenter understøtter design, udvikling og anvendelse af offentlige it-systemer, der

— (gen)anvender oplysninger i form af data og dokumenter til sagsbehandling eller selvbetjening
— sender eller modtager meddelelser fra andre it-systemer

Dokumentet er primært målrettet it-arkitekter tilknyttet offentlige digitaliseringsprojekter, herunder enterprise-arkitekter, forretningsarkitekter og løsningsarkitekter, der har til opgave at kravspecificere og designe løsninger.

De første dele af dokumentet (Strategisk og Forretningsmæssig arkitektur) henvender sig endvidere til projektledere og beslutningstagere, herunder forretningsansvarlige, digitaliseringschefer, it-chefer, afdelings- og kontorchefer og andre med rollen som systemejer.

Dokumentet i sin helhed er også relevant for leverandører at orientere sig i.

1.2 Scope

Referencearkitekturen beskriver anvendelse af og udvikling af it-systemer, der reguleres af blandt andet:

EU databeskyttelse

lov som beskriver pligter og rettigheder ved behandling af persondata

EU eIDAS

lov som definerer registrede tillidstjenester

Persondatalov

lov som beskriver pligter og rettigheder ved behandling af persondata

Lov om Digital Post

lov der gør det obligatorisk for virksomheder og borgere at modtage digitale meddelelser fra offentlige afsendere.

Referencearkitekturen skrives på baggrund af den fællesoffentlige digitaliseringsstrategi 2020 under initiativ 8.1 med tilslutning fra FM, UFM, EVM, SIM, JM, EFKM, MBUL, SÆM, SKM, MFVM, BM, KL og Danske Regioner. Heri beskrives referencearkitekturen således:

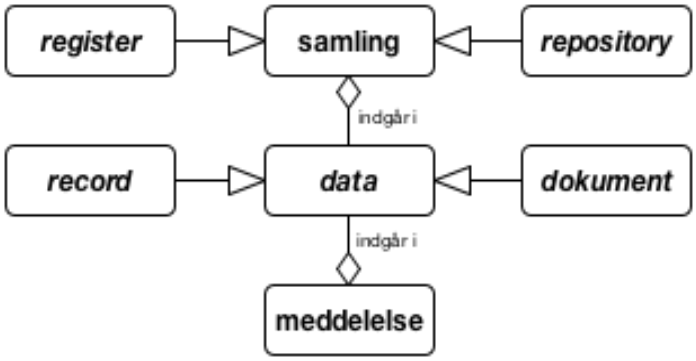
> For at operationalisere, hvilke krav hvidbogen konkret stiller til initiativer og systemer udarbejdes en referencearkitektur for deling af data og dokumenter, der blandt andet beskriver fælles behovsmønstre og mønstre for teknisk understøttelse, herunder de forskelige roller, der skal afklares i initiativerne. Referencearkitekturen udpeger også eventuelle områder for eksisterende og nye fælles standarder og infrastruktur, som skal lette initiativernes implementering. Referencearkitekturen bliver således en generel ramme og støtte for alle initiativernes egen specifikke arkitektur.

Uden for scope af denne referencearkitektur er:

— registrering og intern anvendelse af data hos registerejer
— åbne data, der ikke kræver adgangskontrol (se issue #9)
— streaming (se issue #2)

1.3 Centrale begreber

I det efterfølgende vil begrebet data blive brugt til at betegne både oplysninger på dokumentform og oplysninger der optræder i registre. Vi anvender begrebet datasamling både om et register og et repository med dokumenter.



Figur 1 Anvendelse af begrebet data og relaterede begreber i denne referencearkitektur

Vi vil endvidere lave en skelnen mellem:

— Anvendelse af udstillede data - typisk via API i system-til-system-integrationer
— Forsendelse af meddelelser indeholdende data (herunder dokumenter) - typisk brugt ved beskeder til borgere/virksomheder, der skal have retsvirkning, men også et klassisk mønster brugt i system-til-system-integrationer.

Den fundamentale forskel på disse to scenarier er, om det er afsenderen eller modtageren af data, der kender formålet med interaktionen. Ved udstilling af data er dataafsenderen som udgangspunkt ikke bekendt med datamodtagerens formål (men er naturligvis forpligtet til at håndhæve relevant hjemmel). Ved forsendelse af meddelelser er det dataafsenderen, der i en given kontekst afsender en meddelelse med et givent formål - typisk som led i en proces.

1.4 Anvendelse

Referencearkitekturen skal:

— danne et fælles sprog til at formulere en fælles handlingsplan
— bruges som reference ved løsningsbeskrivelser

1.5 Tilblivelse og governance

Første udgave er skrevet hos Kontor for Data og Arkitektur af Mads Hjorth, Digitaliseringsstyrelsen og Anders Fausbøll, Omnium Improvement.

Endelig godkendelse forventes hos Styregruppe for Data og Arkitektur under Digitaliseringsstrategien 18. december 2017.

1.6 Metoderamme

Referencearkitekturen er udarbejdet inden for rammerne af Fællesoffentlig Digital Arkitektur og følger så vidt muligt den fælles skabelon for referencearkitekturer som udarbejdet i DIGST/KDA. Metoderammen bygger blandt andet på erfaringer fra OIO referencearkitektur, og indarbejder også elementer fra EIRA, TOGAF, ArchiMate m.m.

I dokumentets tekst er særlige elementer angivet i *kursiv* (fx *lov*, *mål*, *rolle* m.m.). Dette markerer, at de hører til Archimate-begrebsapparatet. Andre elementer er angivet med særlig markering. Her er der tale om referencer til begreber/elementer fra figurer. Det bemærkes, at prefixet 'data-' kan være udeladt på begreber/elementer i tekst og figurer fx af formatterings- eller læsbarhedshensyn uden, at der ligger en indholdsmæssig skelnen bag (fx dataanvendelse/anvendelse, datasamling/samling o.a.)

I figurer markerer:

— *Kursiv*: At et element eller en relation ikke er nærmere defineret i denne rammearkitektur (fx dokument)
— Blå tekst: At et element eller en relation ejes og defineres i denne rammearkitektur (fx anvendelse)

1.7 Relation til andre referencearkitekturer

Denne referencearkitektur gør brug af:

— Fællesoffentlig referencearkitektur for brugerstyring

Den skal kunne anvendes af:

— Fællesoffentlig referencearkitektur for selvbetjening
— Fællesoffentlig referencearkitektur for overblik over egne sager og ydelser

... og skal anvendes i kontekst sammen med:

— Deling af dokumenter på sundhedsområdet
— Sag- og dokument på det kommunale område
— Indberetning til registre på sundhedsområdet (under udarbejdelse pr. oktober 2017)

2 Strategisk arkitektur

Udarbejdelsen af referencearkitekturen tager udgangspunkt i en række identificerede forretningsmæssige og teknologiske trends og tendenser.

2.1 Forretningsmæssige tendenser

— Nationalt ønske om at undgå knopskudte løsninger
— Data har øget værdi for organisationer
— Øget bevågenhed omkring beskyttelse af privatliv
— Øget opmærksomhed om håndtering af personlige oplysninger
— Mængden af oplysninger der håndteres stiger
— Grænseoverskridende services

2.2 Teknologiske tendenser

— øget central standardisering af begreber, datamodeller og grænseflader
— Flere og mere forskelligartede enheder forbundet til netværket
— Øgede forventninger til brugervenlighed af offentlige digitale services
— Mængden af tilgængelige oplysninger vokser
— Arkitekturvision for anvendelse og udstilling
— Integrated Service Delivery
— "Interoperability/Samarbejdende infrastrukturer / Økosystem af fælles løsninger?"
— "Valgfrihed for anvender mellem flere tekniske udbydere af samme oplysninger"

2.3 Strategiske målsætninger

De overordnede målsætninger for denne referencearkitektur kobler alle til visionen om det datadrevne samfund, hvor data ses som et råstof for samfundsudviklingen.

Målsætningerne inkluderer:

Interoperabilitet

mål om sammenhængende services... integrated service delivery

Once-only

mål om at borger og virksomhed kun skal afgive den samme information til det offentlige en gang... (men give lov til genbrug?)

Transparens

mål om at borgere og virksomheder skal kunne se, hvilke data der findes om dem, og hvor disse data anvendes

Genbrug

mål om genbrug af it med henblik på lavere omkostninger

2.4 Vision

Visionen i denne referencearkitektur er at stræbe efter en situation, hvor:

> *Data er en fælles, værdifuld og velbeskyttet ressource, som skal være nemme at dele og bruge, men svære at misbruge*

2.5 Værdiskabelse

Værdien ved at følge denne referencearkitektur er, at den giver:

- Mindre besvær for borger og virksomheder ved brug af digitale services
- Simplere arbejdsgange og mere potentiale for automatisering hos organisationer (myndigheder/virksomheder)
- Understøttelse af værdiskabende innovation (ved at gøre data til et 'råstof' for vækst/skabelse af konkurrencefordele)
- Understøttelse af transparens og dermed bevarelse af tillid til registre
- Effektiv systemudvikling (begrænser udfaldsrum, opsamler best practice)

2.6 Strategiske principper

Forretningsmæssige, Informationsmæssige, Applikationsmæssige og Tekniske principper bag referencearkitekturen:

F1: Byrden i datadeling skal afløftes fra dataejer, hvis den begrænser genbrug
F2: Autoritative registre med henvisninger til andre registre
F3: Ansvar for begrænsning af adgang ligger hos registerejer
F4: Data beskrives, fordeles, forbedres og beskyttes i fællesskab
F5: Beskrivelse af, adgang til og brug af data sker under klar governance og håndhæves ud fra tydelig hjemmel
I1: Fælles referenceinformationsmodel
I2: Dokument-princip (attester mv.)?
A1: Onlineopslag i sagsbehandling og selvbetjening
A2: Log adgang
A3: Adgang til og fra internationale registre sker gennem national gateway
T1: Central fuldmagts-/rettighedsstyring
T2: Multi-flavour-api
T3: Fælles metoder for datadeling understøtter sammenstilling af data og tværgående brug blandt myndigheder og virksomheder

3 Forretningsmæssig arkitektur

3.1 Aktører

De væsentligste aktører, der er i spil omkring deling af data og dokumenter, er:

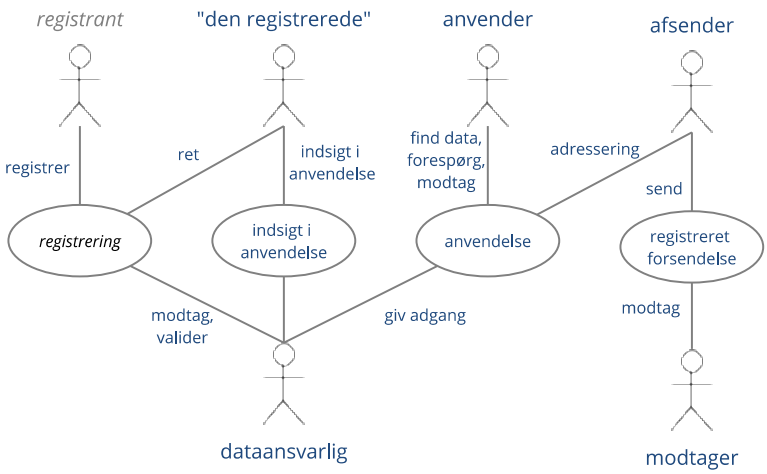
- Offentlige myndigheder, herunder virksomheder, der handler på vegne af offentlige myndigheder
- Borgere
- Virksomheder

3.2 Forretningstjenester og funktioner

Forretningsmæssigt set finder referencearkitekturen anvendelse i løsningen af alle offentlige opgaver. Specifikt kan nævnes nedenstående sæt af generiske procesmønstre:

- Myndigheders sagsbehandling (fra Referencearkitektur for Sag og dokument)
- Selvbetjening, vendt mod borgere og virksomheder (fra Referencearkitektur for Selvbetjening)
- Indsigt i oplysninger og deres anvendelse (fra Referencearkitektur for Overblik over sag og ydelser)
- Sende meddelelse (inkl. brug af tilmeldingslister og påmindelser)
- Modtage meddelelse
- Tag et dokument med til en anden service provider, der ikke har adgang til registre - herunder beskrive, hvordan dokumenter valideres.
- Tværgående analyse, tilsyn og kontrol

Referencearkitekturen kredser om fire centrale, delte *use cases*, hvor aktører arbejder sammen i forskellige roller.



Figur 2 Tværgående use cases og funktioner hos de enkelte roller

De fire use cases er:

Registrering
collaboration hvor oplysninger bringes på digital form

Indsigt i anvendelse
collaboration hvor en borger får indsigt i anvendelse af personlige data

Anvendelse (af udstillede data, herunder dokumenter)
collaboration hvor oplysninger anvendes i en opgave

Registreret forsendelse
collaboration hvor meddelelser sendes uafviseligt

3.3 Forretningsroller
I ovenstående use cases indgår disse forretningsroller:

Registrant
rolle som bringer oplysninger på digital form, registrer

"Den registrerede"
rolle den person (datasubjekt), som oplysningerne vedrører

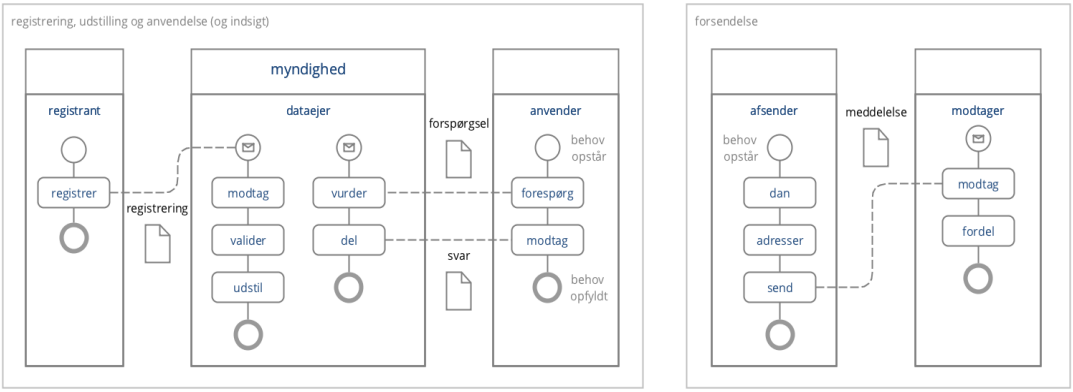
Anvender
rolle der anvender data/oplysninger fra et register

Dataansvarlig
rolle som ejer registreringer/data og har ansvar for at udarbejde adgangspolitik

Afsender
rolle som genererer og afsender meddelelser til en specifik modtager

Modtager
rolle som modtager en meddelelse fra en specifik afsender

3.4 Tværgående processer



Figur 3 Overblik over centrale processer og deres aktiviteter fordelt på roller

Figuren ovenfor beskriver de væsentligste trin i de overordnede procesflow for de fire delte use cases. I denne sammenhæng skal følgende fremhæves:

Registrering

proces En registrant initierer processen ved at registrere ny data hos den dataansvarlige (der er ansvarlig for sikring af hjemmel og håndhævelse af adgangspolitik ifm. registreringen). Når data er korrekt registreret, skal det markeres som klar til at blive udstillet. Her kan der være forskel på, om data gøres tilgængeligt øjeblikkeligt eller først på et senere tidspunkt (fx ved registrering af fremtidigt skift af adresse) - begge muligheder kan være relevante, afhængig af dataanvenders behov.

Indsigt i anvendelse

proces - beskrivelse TBU

Anvendelse af udstillede data

proces Denne proces initieres hos dataanvender - typisk en myndighed, men kan også være en virksomhed - ud fra en startsituation defineret ved, at man har erkendt et behov for data. Dataanvender sender en forespørgsel på data, der beskriver dels, hvilke data, der ønskes, og dels med hvilken hjemmel. Dataansvarlig håndhæver på denne baggrund adgangskontrol, inden data deles og sendes i et svar til dataanvender. Slutsituationen bliver, at dataanvenders databehov er opfyldt. Dataansvarlig er ikke nødvendigvis klar over, hvilket databehov forespørgslen har tjent til at tilfredsstille - så længe, adgangen er legitim og foretaget på baggrund af gyldig hjemmel, kender dataansvarlig ikke nødvendigvis formålet med dataanvenders brug af data i den konkrete forespørgsel.

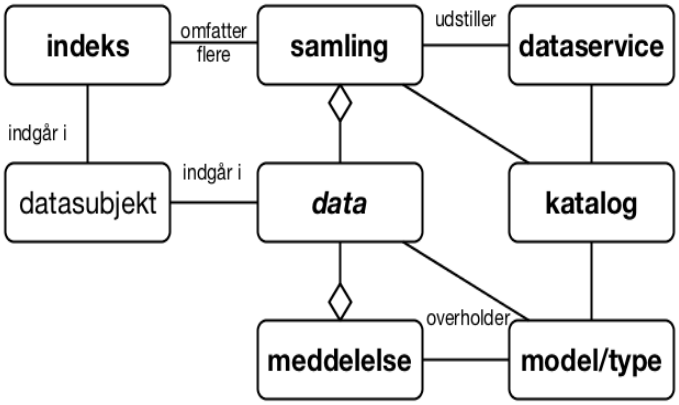
Registreret forsendelse

proces Til forskel fra Anvendelse af udstillede data starter denne proces hos afsenderen (der tillige kan være dataansvarlig). Afsender har udvalgt og pakketeret data i en meddelelse (evt. helt eller delvist i form af et dokument), adresserer meddelelsen (fx ved brug af et kontaktregister) og sender den herefter til modtager. Modtager kan være alle typer af aktører; for myndigheder og virksomheder bemærkes, at det i forbindelse med modtagelsen kan være relevant at fordele/route meddelelsen internt ud fra dens adresseringsoplysninger. I sammenligning med Anvendelse af udstillede data er det nu afsender, der som den part, der deler data, 'ejer' den fulde forretningskontekst - hvor den dataansvarlige ovenfor ikke var bekendt med formålet med at dele data.

3.5 Forretningsobjekter

Nedenfor fremgår en initiel oversigt over en række forretningsobjekter, der er væsentlige for referencearkitekturen.

Regibemærkning for version 0.3: Det videre arbejde skal klarlægge, hvilke elementer der skal indgå i listen, samt hvordan de defineres. Modelleringsniveauet skal endvidere lægges fast (begrebsmodellering og/eller logiske kernemodeller?) Kommentarer og midlertidige bemærkninger indgår i listen, markeret med kantede parenteser.



Figur 4 Oversigt over de centrale forretningsobjekter og deres relationer

data
objekt (Abstrakt. Bruges om både register-record og dokument)

samling
objekt [Datasætmodel har ikke definition...] ISO9115: en identificerbar samling af oplysninger (samlebetegnelse for PSI, GPDR,)

meddelelse
objekt [NgDP] registreret forsendelse

datasubjekt
objekt [Grunddata, fx person. GPDR: den registrede]

model/type
objekt [Jf. modelregler fra FDA]

katalog
objekt [jf hvidbog] både data, service... til design

dataservice
objekt webservice med adgang til datasamling

og andre mulige

registeroplysning
objekt en record

dokument
objekt [Dokumentmodel fra OIO]

påmindelse
objekt [Næste generation Digital Post]

registreringshændelse
objekt

forretningshændelse
objekt

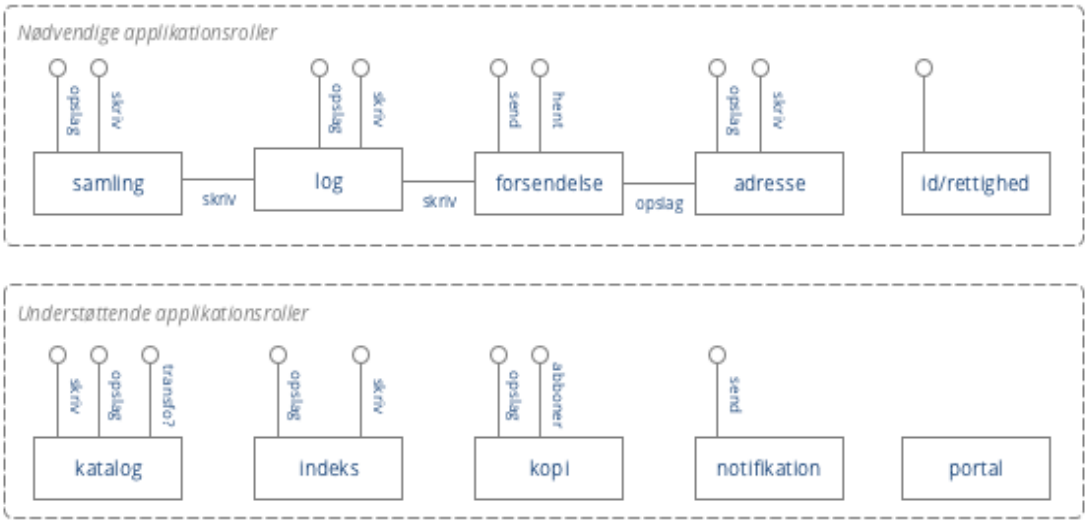
klassifikation
objekt

4 Teknisk arkitektur

Dette afsnit beskriver roller og implementeringsmønstre, der er relevante, når forretningsfunktionerne beskrevet ovenfor skal understøttes/realiseres af applikationer. Endvidere udpeges områder, der er kandidat til standardisering og/eller profilering i forbindelse med reference-arkitekturen.

4.1 Applikationsroller

De nødvendige og understøttende applikationsroller og deres indbyrdes relationer er vist i figuren nedenfor. Nødvendige roller udbyder det minimale sæt af services, der er i spil i en datadelingsarkitektur. Undersøttende roller udbyder services, der i mange situationer vil være fordelagtige at implementere for at øge tilgængelighed, performance, brugervenlighed m.m. i en given datadelingsløsning.



Figur 5 Oversigt over nødvendige og understøttende applikationsroller

Datasamling (dataservice?)

applikationsrolle som har til ansvar at opbevare en datasamling, udstille denne og begrænse adgangen til den om nødvendigt

Når datasamlingen udgøres af dokumenter kaldes den nogle gange et repository, ellers kaldes den også et register. Data kan skrives og fremsøges igen ved opslag. Samlinger kan have temporale og bitemporale egenskaber. Dette handler blandt andet om at holde styr på datas gyldighedsperiode og registreringstidspunkt for fx at kunne understøtte dobbelt historik (overblik både over, hvad der var korrekt på en given dato, og hvad registeret på et givent tidspunkt troede var korrekt på samme tidspunkt).

(Record Management og Data Publication i EIRA)

Log (adgangslog? anvendelseslog?)

applikationsrolle en slags datasamling, der indeholder oplysninger om videregivelse af data fra datasamlinger

Der findes også andre typer af logs, fx skrive-log og validerings-log. I denne sammenhæng er fokus på logning af de data, som en registreret har ret til at få oplyst.

(Logging, EIRA)

Forsendelse

applikationsrolle der kan modtage og distribuere meddelelser

(Messaging og Registered Electronic Delivery, EIRA)

Adresse

applikationsrolle en slags datasamling (fx et kontaktregister), der indeholder oplysninger til brug ved adressering af meddelelser

(Capability Lookup og Service Discovery, EIRA)

Id/Rettighed (Brugerstyring?)

applikationsrolle der anvendes til identifikation af brugere og tildeling af rettigheder (?)

(Identity Management og Access Management, EIRA)

Katalog

applikationsrolle en slags datasamling, der beskriver en given datasamling. Anvendes typisk på design-tidspunktet.

Der findes kataloger over mange ting: services, datasæt, systemer, datamodeller, dokumenttyper...

Indeks

applikationsrolle en slags datasamling, der indeholder oplysninger om, hvilke datasamlinger der indeholder oplysninger om personer, virksomheder og andre forvaltningsobjekter. Et Indeks har typisk til formål at effektivise søgning og fremfinding

Kopi

applikationsrolle en datasamling, som er en direkte kopi af den dataansvarliges autoritære datasamling

Den kan have en abonnementsservice, så anvender kan abonnere på ændringer i datasamlinger.

(Data Publication Service i EIRA)

Notifikation

applikationsrolle der udsender notifikationer/påmindelser.

(Messaging, EIRA)

Portal

applikationsrolle der udstiller digital selvbetjening rettet mod en særlig målgruppe, fx borgere eller virksomheder

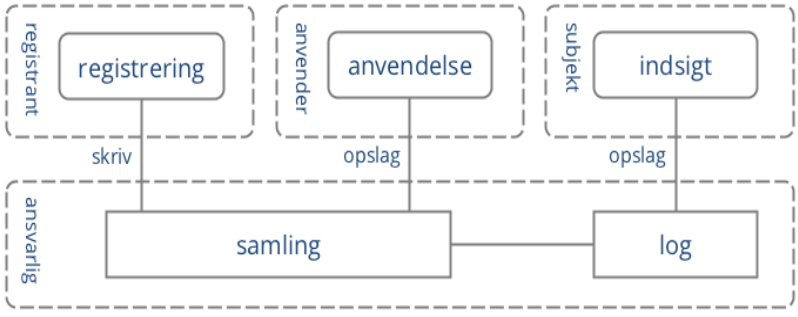
4.2 Tekniske Implementeringer

Her grupperes de enkelte forretningsroller og applikationsroller i forskellige implementeringsmønstre.

4.2.1 Anvendelse af udstillede data

Når en dataanvender (virksomhed eller myndighed) vil have adgang til data hos en dataansvarlig myndighed, kan det ske via ét af nedenstående tre mønstre:

Direkte adgang

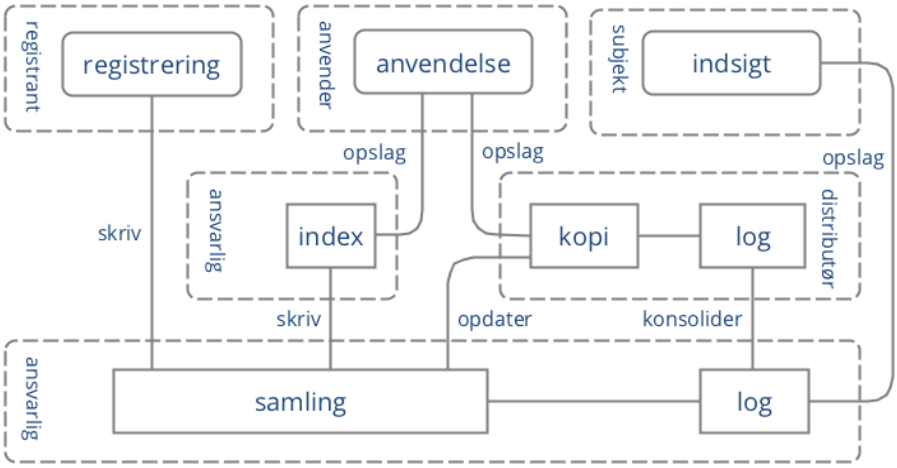


Figur 6 Implementeringsmønster med direkte adgang til registre

I dette mønster, som er simpelt og måske det mest klassiske, er det dataansvarlig, der selv udstiller data til de mulige anvendere via en service-orienteret arkitektur. Dataansvarlig er også ansvarlig for at betjene datasubjektets forespørgsler om datansvarligs brug af personlige data.

Fordelen ved dette mønster er, at det er simpelt. Ulempen er, at dataansvarlig kommer til at bære hele udgiften ved at stille data bredt til rådighed.

Datadistribution



Figur 7 Implementeringsmønster for datadistribution

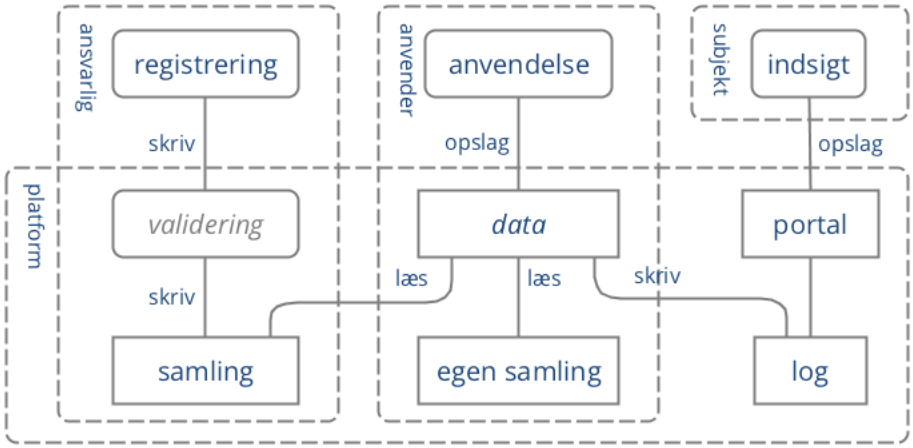
I dette mønster er dataansvarlig fortsat ansvarlig for at tilbyde en service til registrering af data. Anvendelsesdelen er imidlertid afløftet til en datadistributør (evt. flere). Dette giver datadistributøren mulighed for at fokusere netop på distributionen, dvs. at gøre data bredt tilgængeligt (dog naturligvis under håndhævelse af adgangskrav specificeret af dataejer) til dataanvendere.

Når nye data registreres, har dataansvarlig ansvaret for at opdatere kopien af datasamlingen hos datadistributøren.

I det tilfælde, hvor ensartede datasamlinger ligger hos flere, separate dataansvarlige - eksempelvis sundhedsdata opbevaret i forskellige regioner - er det fordelagtigt at anvende et index for at sikre effektive opslag. Dataansvarlig opdaterer dette index, når en registrant opdaterer datasamlingen.

Logningsmæssigt er den enkelte distributør ansvarlig for at logge dataanvenders adgang til data. Samtidig er den enkelte distributør ansvarlig for at sørge for konsolidering af loggen for at sikre, at datasubjekt har adgang til information om anvendelse af data om vedkommende selv. I figuren er log-konsolidering lagt hos dataansvarlig, men den kunne i princippet også være uddelegeret - så længe, der er et entydigt og klart *single point of contact* for datasubjektets opslag i anvendelsen af personlige data.

Distribueret service- og data-platform



Figur 8 Implementeringsmønster for distribueret dataplatform

Delingsansvaret er i dette mønster i høj grad håndteret af en dataplatform. Platformen er distribueret og er i stand til at replikere data på tværs af dataansvarligeog dataanvendere. Dvs., at data, der registreres via en dataansvarlig myndighed, gøres tilgængelige for andre, dataanvendende myndigheder via platformen.

Da dataplatformen kan rumme data fra mange forskellige dataejere, muliggøres effektiv sammenstiling af data hos dataanvenderen, der kan kombinere data fra egne samlinger med data fra andre samlinger. Data kan her forstås både som simple opslag i egne eller andres datasamlinger, og som sammenstillinger, hvor data fra flere samlinger kombineres for at servicere dataanvenders applikationer.

Platformen er ansvarlig for at håndhæve adgangskontrol, herunder at sikre, at anvendelsesapplikationer har den nødvendige lovhjmmel til at tilgå en given, distribueret samling. Eventuelle services hos dataanvender, der gør brug af data, er ansvarlige for at logge deres brug. Platformen konsoliderer brugs-loggen og gør det muligt for datasubjekt at få overblik over brug af personlige data.

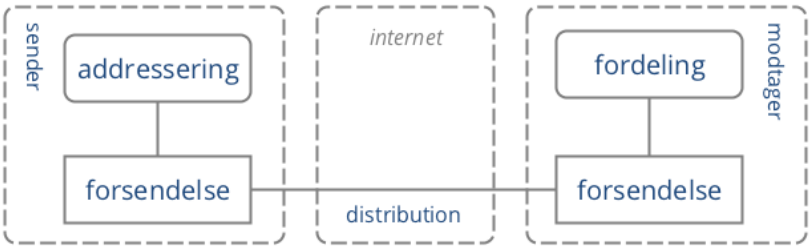
Fordelen ved dette mønster er den umiddelbare og standardiserede tilgænglighed til data, som en dataplatform kan levere. Ulempen er, at kompleksiteten øges, samt at der stilles større krav til dataanvenders modenhed ift. den tekniske adgang til data (da dataanvenders applikationer i praksis vil skulle afvikles på den distribuerede Service- og Dataplatform).

(Uafklaret: Skal Dataanvenders applikationer/services have direkte adgang til distribuerede data, eller skal adgang fortsat ske via et servicesnit, der kan varetage adgangskontol m.m.? Tracket i issue 7.)

4.2.2 Registreret forsendelse

Når en myndighed vil initiere en specifik og målrettet datadeling - dvs. sende data (herunder dokumenter) til en anden myndighed, virksomhed eller borger - kan det ske via ét af de tre nedenstående mønstre.

Sikker e-mail

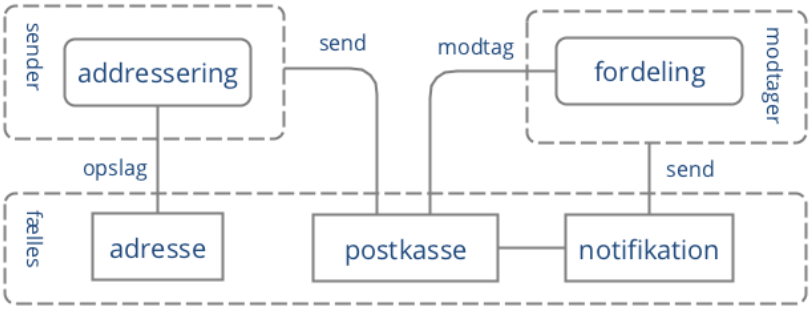


Figur 9 Implementeringsmønster for Sikker e-mail

Et meget anvendt mønster for myndighed til myndighed-kommunikation er at levere en meddelelse fra afsender til modtager gennem forsendelse brug af sikker e-mail. Ud over at påpege, at distributionen her sker via en sikker og krypteret forbindelse, faldet detr uden for dette dokuments scope at beskrive dette mønster yderligere. Det er dog medtaget for reference pga. dets brede anvendelse. Det er endvidere oplagt at betragte dette mønster som et særtilfælde af det generelle 'Service provider'-mønster nedenfor.

Fordelen ved dette mønster er, at det er simpelt og benytter sig af standardteknologi. Ulempen er, at det kun dækker myndighed til myndighed-kommunikation. Derudover sætter standardteknologien (e-mail) visse begrænsninger for funktionalitet, der fx understøtter fordeling(automatisk routing) af beskeder hos modtagende virksomhed/myndighed i det tilfælde, hvor meddelelsen ikke har én specifik modtager.

Fælles system



Figur 10 Implementeringsmønster for fælles system

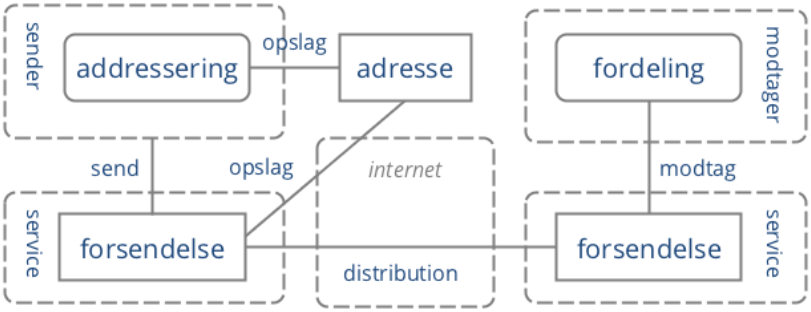
Ved brug af Fælles system-mønsteret til forsendelse af en meddelelse benytter afsender og modtager et centralt, fælles postkasse til hhv. at placere meddelelsen og læse den. I den analoge verden svarer dette mønster til, at afsender og modtager benytter et fælles postbokskontor. Digitalt er dette mønster fx implementeret af Digital Post, hvor såvel myndigheder, virksomheder og borgere kan placere meddelelser, der efterfølgende kan hentes af modtager. Også messaging-funktionaliteten i mange af de sociale medieplatforme (fx Facebook) falder i denne kategori.

TIl forskel fra Sikker e-mail-mønsteret ovenfor er Fælles system-mønsteret mere robust, både da adresseringsservicen tilbyder opslag/verifikation mod et adresseregister, samt da meddelelsen opbevares i infrastrukturen, indtil modtager aktivt læser den - i modsætning til Sikker e-mail, hvori infrastrukturen blot videresender meddelelsen og dermed er afhængig af, at modtageren i praksis findes.

Postkassefunktionaliteten har endvidere mulighed for at trække på en notifikationsservice, der kan tilbyde indholdsreducerede notifikationer til modtager om den nye meddelelse.

Et Fælles system-mønster kan fungere på mange niveauer, herunder nationalt (fx Digital Post); inden for et specifikt domæne, fx på sundhedsområdet; eller rent bilateralt, hvor to organisationer enes om dette mønster og vælger en passende meddelelsesplatform.

Økosystem/Service providers



Figur 11 Implementeringsmønster for økosystem

I dette mønster deltager både afsender (A) og modtager (D) i et meddelelses-økosystem ved at vælge hver sin Forsendelses-Service provider (hhv. B og C). Økosystem-mønsteret er bl.a. kendt i kontekst af den europæiske eDelivery-standard som en *four corner model*.

Et fælles adresseregister/kontaktregister udgør en central komponent i økosystemet, der gør det muligt for alle parter at slå den relevante adresseringsinformation op. En afsender kan via adresseregisteret se/verificere mulige modtagere, samt evt. afgøre hvilken konkrete meddelelsesformater/kanaler, modtager kan håndtere. Forsendelsesservicen, der håndterer afsendelse af Meddelelsen, kan benytte adresseregisteret til at finde modtagerens konkrete Service provider og bliver dermed i stand til at levere meddelelsen.

Mønsteret vil typisk være symmetrisk, således at en afsender også kan indgå som modtager og vice versa. Mønsteret kan i øvrigt både være generisk eller specifikt for et domæne, der fx kan stille ekstra krav til meddelelsens format.

Fordelene ved Økosystem-mønsteret er, at det er robust, fleksibelt og løbende kan udvides med nye Service providers. Ulempen er, at der stilles store krav til det centrale adresseregister, samt at der fortsat ikke findes standardteknologier, der dækker mønsteret.

4.2.3 Registrering

Registrering af data er ikke i scope for denne referencearkitektur, men medtages kort pga. sin væsentlige relation til Indeks-konceptet.

Opdateres.

Ansvar hos registrant

implementationsmønster

Ansvar hos dataejer

implementationsmønster

Ansvar hos distributør

implementationsmønster

4.3 Integrationer

I de ovenstående implementeringsmønstre for hhv. Anvendelse af udstillede data og Registreret forsendelse indgår der en lang række relationer mellem de beskrevne elementer. Relationerne dækker i praksis over integrationer mellem to applikationer. Nedenfor opridser vi de relationer, der er væsentlige for denne referencearkitektur. Alle relationer er ikke relevante i vores kontekst - men sagt populært, hvis der "står noget på en linje mellem to kasser", er de mest fremtrædende karakteristika og kendetegn ved den underliggende integration beskrevet nedenfor:

Integrationsbeskrivelser opdateres.

skriv

Med kvittering...

opslag

beskytter mod misbrug, og beskyttet mod DDOS *TBU: DNS*

opdater

Bulk, Delta, Teknologispecifikt

konsolider

Skriv eller høst

læs

SQL eller Fil, men log

distribution

uafviselighed, beskyttet, payload/header

hent meddelelse

TBU

modtag notifikation

borger - SMS/APP

4.4 Områder for standardisering/profileringer

Nedenstående, tekniske områder er kandidater til at indgå i referencearkitekturen i forhold til at pege på en anbefalet standard eller en særlig profilering, evt. vendt mod de enkelte, tekniske mønstre.

Integrationer

— Service Design Guidelines
— Data Write Protocols

— Data Access Protocols
— Distribution Protocols
— Notification Protocols
— Synchronisation Protocols

Indholdsmæssige standarder

— Metadata for opslag/søgning/anvendelse
— Log format
— Hjemmel (samtykke, lov)
— Kontekts (klassifkation af anvendelse)
— Hændelsesbeskeder
— Identifikation
— Klassifikation af følsomhed

4.5 Identifikation af eksisterende standarder

TBU.