e-oppslag, modell over aktører og komponenter

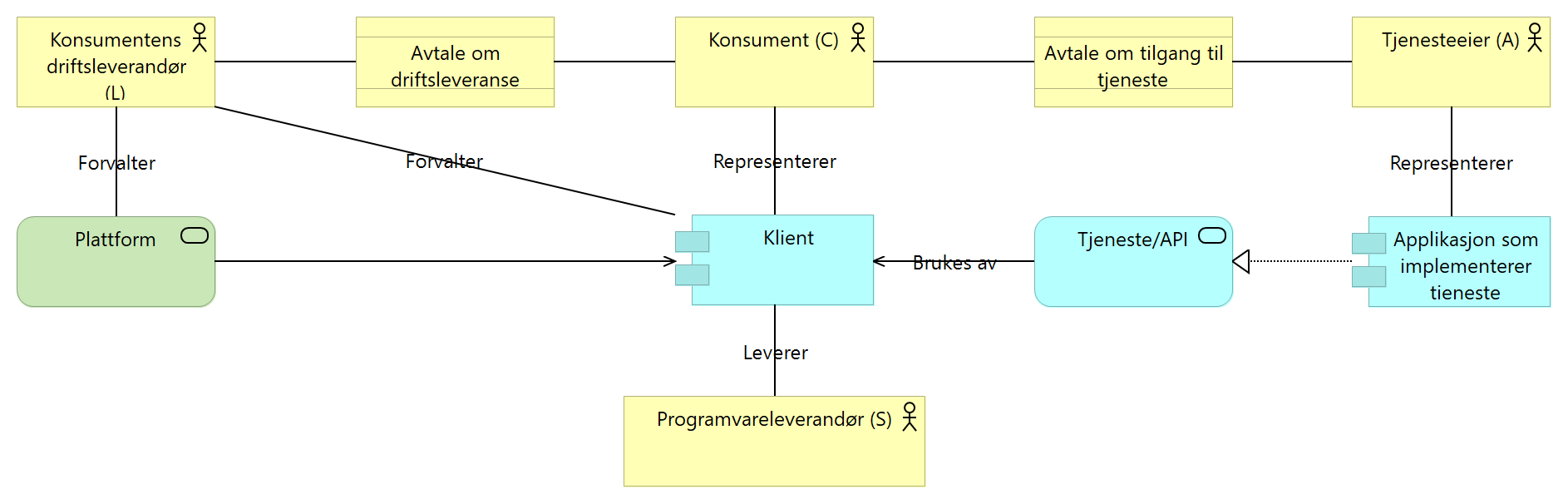
Av: Rolf Rander Næss, Acando AS, for Brønnøysundregistrene

Dato: 2018-05-23

# Aktører og komponenter

Figuren er i «archimate»-notasjon. Dette skal ikke være noen lærebok i archimate, men jeg forklarer hva de ulike figurene betyr i omtalen av hver enkelt nedenfor.

I denne modellen er token-tjenesten som gjør autentisering bevisst utelatt. Denne figuren skal vise det som inngår i målsetningen. Token-tjenesten er et middel for å oppnå kommunikasjon, ikke et mål i seg selv.



## Aktører

En aktør er notert i archimate som en gul boks med en strekfigur. Vi diskuterte 4 ulike typer aktører, bokstavene i parentes er de vi brukte i figurene på tavla:

* Tjenesteeier (A): den part som tilbyr en tjeneste gjennom et API
* Konsument (C): den part som skal bruke tjenesten og juridisk sett er mottaker
* Konsumentens driftsleverandør (L): en separat organisasjon som konsumenten bruker til å forvalte deler av eller hele sin tekniske infrastruktur, samt som i større eller mindre grad er integrert i konsumentens forretningsprosesser. Her begynner det å bli vanskelig, fordi det finnes (minst) tre ulike modeller og det er utydelig hvor grensene går:
  1. C og L er samme organisasjon (eller L sin rolle er ubetydelig i denne sammenhengen): her kan man se bort fra de tre boksene til venstre i figuren (leverandør, plattform, og avtalen med leverandøren) og det hele blir mye enklere
  2. L er en sky-leverandør, men C forvalter klienten selv (for eksempel: C kjøper programvare fra Visma og installerer i Azure. I denne sammenhengen er Microsoft en «databehandler», men fra A sitt perspektiv er L usynlig)
  3. L leverer en integrert tjeneste til C, typisk i en eller annen slags delt løsning, men hvor vi typisk ønsker at L autentiseres som seg selv, men er autorisert til å opptre på vegne av flere C. (for eksempel: Eika opptrer på vegne av 57 banker, et regnskapskontor opptrer på vegne av sine kunder)
* Programvareleverandør (S): der hvor konsumenten (C) ikke går gjennom en driftsleverandør, men integrerer direkte vil det i mange sammenhenger ikke være C som lager programvaren, men de kjøper for eksempel et ERP-system fra en leverandør, og dette kaller tjenesten. Hvorvidt S er relevant i tilgangsstyringen vil variere.

## Avtaler

En avtale i archimate-notasjon er en gul boks med to vannrette striper. Det er to avtaler involvert som er relevant:

* Avtale mellom konsument (C) og driftsleverandør (L). Dersom L skal opptre på vegne av C (scenario 3 over) er det denne avtalen som delegerer myndighet fra C til L.
* Avtale mellom tjenesteeier (A) og konsument (C). Dette er den avtalen som regulerer C sin tilgang på opplysninger/tjenester fra A. I vår sammenheng hvor C og/eller A er offentlige virksomheter vil denne avtalen typisk være strengt regulert i lov og forskrift.

## Applikasjonstjenester og -komponenter

Alle begrep på applikasjonslaget er turkis i archimate-notasjonen. Bokser med runde hjørner er tjenester/API, bokser med to «kontakter» til venstre er komponenter.

* Klient: dette er omtrent det samme som «client» i OAuth, altså den komponenten som ønsker tilgang til en ressurs
* Applikasjon som implementerer tjeneste: jeg *tror* dette er det samme som «resource server» i OAuth.
* Tjeneste/API: grensesnittet som realiseres av «resource server» og som brukes/konsummeres av «client»

Pilene betyr:

* Åpen pil: «brukes av»
* Trekant med stiplet linje: «realiserer»

# Scenarier

Diskusjonene våre dreier seg om ulike scenarier, og vi har litt problemer med å skille dem fra hverandre i diskusjonen. Dette er de jeg ser, med eksempler (jeg har begrenset utvalget litt sammenlignet med tidligere notater):

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario navn | Typisk antall konsumenter | Typisk antall tjenesteeiere | Beskrivelse |
| Lovhjemlet | 1-10 | 1 | Utveksling av informasjon mellom offentlige etater hvor dette er spesifikt hjemlet i lov og forskrift, og hvor den aktuelle informasjonen typisk inngår i definerte prosesser hos alle involverte parter. Et eksempel er utlendingsforvaltningen som er fordelt mellom Politiet, UDI og UNE, og hvor disse utveksler bestemte opplysninger på definerte steder i saksgangen. |
| Etter avtale | 10-1000 | 1 | Oppslag på informasjon hvor bruk av informasjonen er begrenset i lov og forskrift, men med en større bredde i konsumenter og bruksområder, samt definerer bredere grupper av konsumenter («alle kommuner» eller «alle banker»). |
| Alle virksomheter | Over 1 million | 1 | Tjenester som alle registrerte virksomheter i prinsippet får lov til å bruke |
| Revers | 1-10 | 10-1000 | Der hvor offentlige etater trenger å kalle tjenester hos private virksomheter for å hente informasjon om disse virksomhetene sine kunder. |

Utenfor scope i denne omgang:

* Virksomhet gjør kall på vegne av en borger
* Utenlandske virksomheter

For alle scenariene hvor det er flere enn 10 aktører må det også støttes at det finnes sentrale leverandører eller bransjeorganisasjoner som opptrer på vegne av flere aktører (for eksempel «eika» på vegne av en rekke banker, eller en regnskapsfører på vegne av sine kunder).

Det finnes kanskje ingen prinsipielle forskjeller mellom «lovhjemlet» og «etter avtale», men antall konsumenter har mye å si for krav til skalerbarhet.

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Eksempel NAV | Eksempel Skatt | Eksempel BR |
| Lovhjemlet |  |  | Informasjon om utleggstrekk mellom Statens Innkrevingssentral og Brønnøysundregistrene. |
| Etter avtale | Pensjonsforsikring? | Samtykkebasert lånesøknad  Oppslag i folkeregisteret | Kredittopplysningsselskap som slår opp i løsøreregisteret |
| Alle virksomheter | Sykelønn? | Hente skattekort | Oppslag eller redigering av egen informasjon i foretaksregisteret |
| Revers | Oppslag hos forsikringsselskap | Oppslag hos banker |  |