Høringssvar vedr. Serviceinterface for Person

1. Indledning

Dette dokument udgør IT Crew's høringssvar til IT- og Telestyrelsens høring vedr. "Specifikation af serviceinterface for Person" med høringsfrist d. 19. august 2011.

1.1 Arkitekturmæssige overvejelser

Helt grundlæggende beskrives en servicefacade, som fagsystemer / ESDH systemer i en myndighed kan anvende mod enten det centrale CPR register eller lokale kopier af CPR registret. Formålet et at standardisere denne snitflade (OIOXML), at muliggøre hændelsesstyret opdatering samt indførsel af nye data (kontaktkanaler).

Specifikationen tager i høj grad udgangspunkt i den bestående verden, hvor data altid leveres af nogle faste, centrale registre, hvilket ikke nødvendigvis vil være gældende i al fremtid. Eksempelvis kan kontaktoplysninger komme fra en lang række forskellige kilder. Vi er bekymrede for, at specifikationen ikke har den fornødne fleksibilitet (og løse kobling) til at kunne håndtere nye registre, nye måder at tilvejebringe oplysninger, nye personoplysninger etc., således at den vil kunne blokere for fremtidig udvikling og innovation.

Vi foreslår derfor, at der arbejdes med at generalisere informationsmodellen, så følgende arkitekturmæssige principper honoreres:

1. Modellen bør gøre det muligt at introducere nye personoplysninger samt nye registre / kilder til personoplysninger – frem for at være låst til de nuværende attributter og registre. Introduktionen af nye registre bør kunne ske via en gradvis proces.
2. Modellen bør kunne operere med multiple datakilder og derfor som konsekvens eksplicit rumme metadata om, hvorfra en oplysning stammer, således at applikationer via politikker kan vurdere, *om* og *hvordan* de vil anvende en personoplysning. Dette princip ses anvendt bl.a. i SAML 2.0 standarden[1] via et *Issuer* begrebet, og det diskuteres pt. i *Kantara Initiative*'s eGovernment gruppe.
3. Der bør være en løsere kobling til CPR registret via et højere abstraktionsniveau / mere generel snitflade, men CPR registret skal naturligvis kunne levere data via den mere generelle snitflade.

Med henvisning til IT- og Telestyrelsen's eget diskussionspapir "Nye digitale sikkerhedsmodeller" vil vi fremhæve følgende vigtige arkitekturprincipper, som ligeledes bør tilgodeses:

4. Data skal kunne flyde mellem systemer *via brugeren* fremfor via direkte system-til-system integrationer, således at brugeren vil kunne være i kontrol.

[1] http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

5. Det er vigtigt, at oplysninger om en bruger kan stamme fra et kontekstafhængigt akkreditiv og således ikke altid være direkte bundet til et CPR nummer (eller andre identificerende nøgler) – men i stedet et *pseudonym*. I modsat fald er det ikke muligt at opnå princippet om transaktionsisolering, hvilket er en central egenskab i forhold til sikkerhed og privacy.

Den ønskede fleksibilitet opnås naturligvis ikke alene ved at generalisere informationsmodellen: applikationerne, der anvender modellen, skal naturligvis også have indbygget en vis fleksibilitet / intelligens, således at de ikke er hard-kodede til det nuværende CPR paradigme.

2. Konkrete ændringsforslag

I dette kapitel gives en række konkrete ændringsforslag til informationsmodellen med henblik på at opnå nogle af de arkitekturmæssige egenskaber, der er beskrevet i sidste kapitel. Grundet begrænsede tidsmæssige rammer til at udarbejde dette høringssvar, har det ikke været muligt at udarbejde et komplet forslag til en helt ny informationsmodel, som realiserer alle de ønskede egenskaber. I stedet bringes en række mindre gennemgribende forslag til den eksisterende informationsmodel.

2.1 Variable attributnavne

I stedet for at operere med specifikke, navngivne attributter, foreslås at man generaliserer modellen, så attributters navne er variable dvs. modelleres som en *identifier* (eksempelvis en URI, som det er tilfældet for attributter i SAML 2.0 standarden). På den måde er modellen ikke låst til et på forhånd defineret sæt af standardattributter.

2.2 Registeroplysninger fra akkreditiv

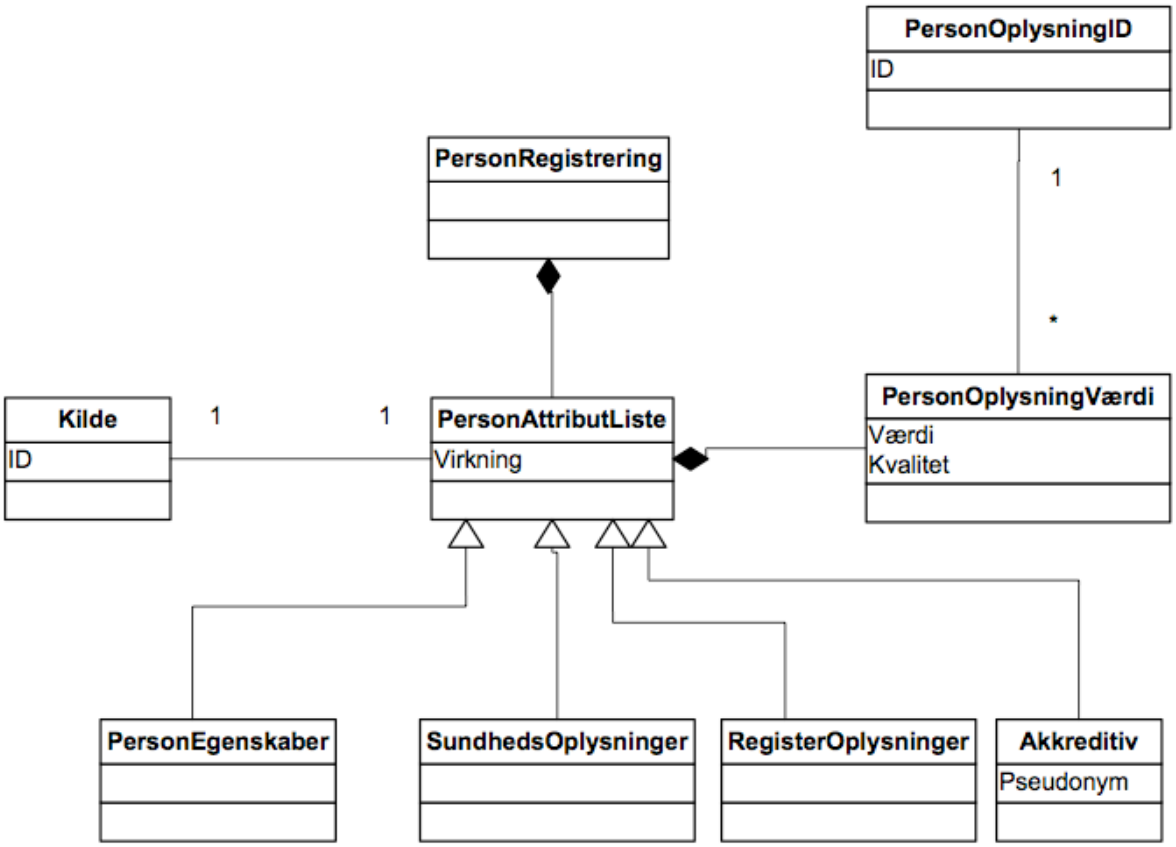
Det foreslås, at der indføres en ny subklasse til "RegisterOplysninger" entiteten, svarende til generelle personoplysninger fra et akkreditiv (herunder kontekstafhængige akkreditiver). Som nævnt ovenfor kan hver type af personoplysning være identificeret via en URI. Klassen *Akkreditiv* kan eksempelvis indeholde en *Pseudonym* attribut for at muliggøre, at personoplysningerne ikke er bundet til et CPR nummer.

2.3 Kilde til og kvalitet af personoplysninger

Det foreslås, at der tilføjes en kildeattribut til personoplysninger (eksempelvis en URI), således at man eksplicit kan modellere, hvorfra en given personoplysning stammer (eksempelvis CPR register, lokalt register, akkreditiv etc.). Ligeledes kan man indføre en attribut, som beskriver i hvor høj grad personoplysningen er valideret dvs. et mål for kvaliteten af de foreliggende data.

2.4 UML eksempel

Nedenfor vises et eksempel på et brudstykke af en UML-model, der indfører de ovennævnte konkrete ændringsforslag.



Som eksempel kan en *PersonOplysningID* udpege typen af personers efternavne via en URI som f.eks. "urn:oid:2.5.4.4" eller "dk:gov:attribute:surname". En *PersonOplysningsVærdi* er så en konkret værdi af denne type, eksempelvis Værdi="Jensen" – og værdien kan have en kvalitet som angivet af *Kvalitet* attributten – eksempelvis "dk:gov:cpr_register_valideret"[2].

Entiteten *PersonAttributListe* udgør en samling af personoplysninger dvs. deres ID'er og tilhørende værdier. De underliggende entiteter (eksempelvis *PersonEgenskaber*) er så blot simple specialiseringer, der hver forventes at indeholde et bestemt sæt personoplysninger.

[2] Disse er blot fiktive URI'er, som selvfølgelig skal defineres.