Styregruppen for data og arkitektur

Reviewrapport for: 7.2 Afprøvning af fælles standarder for sikker information

Indhold

Arkitekturreview (scopereview) af 7.2 Afprøvning af fælles standarder for sikker information

Arkitekturreviewet af 7.2 Afprøvning af fællesstandarder for sikker information er et scopereview og udført på baggrund af projektets fremsendte materialer:

1. Initiativbeskrivelse for 7.2.pdf
2. Initiativ_7.2 – 20170911.docx
3. PID_GB201_fælles_standarder_v0.32.pdf
4. Anvendelsesscenarier - identitetsbaserede serviceintegrationer på sundhedsområdet - v10.docx,
5. Målbilleder - identitetsbaserede serviceintegrationer på sundhedsområdet - v10.docx
6. Målarkitektur - identitetsbaserede serviceintegrationer på sundhedsområdet - v08.docx
7. Konceptuel model_v041.docx
8. Opfyldelse af referancearkitektur_20171113.docx.

Reviewet er udført i overensstemmelse med model for reviews, godkendt af styregruppen for data og arkitektur maj 2017. Reviewboardet og deltagere er listet i nedenstående tabel:

Reviewboard:	Dan Bjørneboe, KL
	Michael Buch-Larsen, Danmarks Miljøportal
Sekretariat for 8.1:	Michael Philip Poulsen, sek.
	Kirsten Taarnskov, sek.
	Lars Thomsen, arkitekt
Projektdeltagere:	Esben Andreas Dalsgaard, arkitekt og projektleder
	Christian Gasser, ekstern konsulent på projektet
	Søren Ærendahl Mikkelsen, ekstern konsulent på projektet

Reviewgrundlag

Udgangspunktet for reviewet udgøres af hvidbog om fællesoffentlig digital arkitektur samt referencearkitektur for brugerstyring. Principper fra hvidbogen er gengivet nedenfor:

1. Arkitektur styres på rette niveau efter fælles rammer (styring)
2. Arkitektur fremmer sammenhæng, innovation og effektivitet (strategi)
3. Arkitektur og regulering understøtter hinanden (jura)
4. Sikkerhed, privatliv og tillid sikres (sikkerhed)
5. Processer optimeres på tværs (opgaver)
6. Gode data deles og genbruges (information)
7. It-løsninger samarbejder effektivt (applikation)
8. Data og services leveres driftssikkert (infrastruktur)

Projektresume

Der er en stigende efterspørgsel fra myndigheder efter at koordinere og sammentænke brugerstyring på tværs af den offentlige sektor. I de senere år er der udviklet fællesoffentlige standarder som fx OIOIDWS, der blandt andet gør det muligt at vise personlige data fra offentlige registre på en sik-

ker og standardiseret måde. Skiftet til fællesoffentlige standarder er undervejs flere steder i den offentlige sektor og ses som en væsentlig trædesten for fremtidig digitalisering.

Det er også tilfældet for sundhedsvæsenet, som i stigende omfang begynder at tilbyde digitale løsninger til borgere og patienter (fx telemedicin). Der indsamles helbredsoplysninger via måleudstyr i hjemmet, og borgerne besvarer spørgeskemaer digitalt. Denne positive udvikling udfordrer imidlertid visse af de sikkerhedsstandarder, som i dag benyttes.

Sikkerhedsstandarderne i sundhedssektoren skal derfor opdateres, hvilket sker igennem en større anvendelse af fællesoffentlige sikkerhedsstandarder såsom OIOIDWS. Dette vil gøre det nemmere at udbygge digitaliseringen af sundhedsvæsenet med tidssvarende teknologiske løsninger og samtidig gøre det nemmere for it-leverandører at byde ind med moderne - og måske billigere - it-løsninger.

Dette projekt har til opgave at udarbejde en profilering af OIOIDWS sikkerhedsstandarder til sundhedsområdet. Efterfølgende skal profilen afprøves i tre pilotprojekter, inkluderende et regionalt sundhedssystem, et kommunalt sundhedssystem og et lægepraksissystem. På baggrund af afprøvningen estimeres de fremadrettede omkostninger ved ibrugtagning af profilen i relevante it-systemer. På baggrund heraf skal der udarbejdes et beslutningsoplæg vedrørende migrering til den nye profil, som fremlægges den Nationale Bestyrelse for Sundheds-it.

Indstilling

Det er reviewboardets vurdering, at 7.2 Afprøvning af fælles standarder for sikker information er i overensstemmelse med principper og regler for den fællesoffentlige arkitektur, som fremstillet i hvidbog om fællesoffentlig digital arkitektur og referencearkitektur for brugerstyring.

Det er reviewboardets opfattelse at retning og scope som udlagt i det fremsendte materiale stemmer godt overens med den vision og de principper, som hvidbog om fællesoffentlig digital arkitektur udtrykker. Dette ses ved, at 6 ud af 8 af hvidbogens principper vurderes i grøn og 1 princip vurderes i gult. Infrastrukturprincippet er ikke vurderet, da det ikke er indenfor rammerne af dette scopereview, og der har derfor heller ikke været inkluderet materiale til reviewet, der har muliggjort en faglig vurdering heraf. Anbefalingerne givet i review-rapporten er udtryk for, hvad reviewboardet vurderer som væsentligt, at projektet forholder sig til i det videre arbejde.

Niveau	Vurdering	
Styring	Fuldt opfyldt	
Strategi	Fuldt opfyldt	
Jura	Delvist opfyldt	
Sikkerhed	Fuldt opfyldt	
Opgaver	Fuldt opfyldt	
Information	Fuldt opfyldt	
Applikation	Fuldt opfyldt	
Infrastruktur	Ikke vurderet	

Reviewbordet har udarbejdet 5 anbefalinger, givet i denne review-rapport.

Alle anbefalinger er til det nuværende projekt. Projektet anmodes om at tage stilling til disse anbefalinger i en handlingsplan.

Der er ikke identificeret tværgående anbefalinger i forbindelse med nærværende review.

Anbefalinger

Reviewet af 7.2 Afprøvning af fælles standarder for sikker information har identificeret en række anbefalinger til projektet.

Projektet anmodes om at imødegå disse ud fra et følg-eller-forklar princip i deres bemærkninger til review-rapporten samlet i en handlingsplan. Anbefalinger og handlingsplan indgår i styregruppen for data og arkitekturs behandling af reviewet.

Anbefalinger til det nuværende projekt

1. Det anbefales, at projektet tydeliggør, hvis der er intentioner om indførelse af standarder ved lovgivning.

Reguleringen på sundhedsområdet giver en ramme for indførelse (og udbredelse) af standarder ved lov. Dette har betydning for måden, hvorpå standarderne indføres og udbredes, herunder i forhold til leverandører. Reviewboardet finder det hensigtsmæssigt, at projektet afklarer og tydeliggør, hvorledes projektet vil tilgå udbredelse.

2. Det anbefales, at projektet tydeliggør, hvordan rammer for henholdsvis domænespecifik, fællesoffentlig og international styring sammentænkes.

Reviewboardet vurderer, at de forskellige styringsrammer inden for et domæne, fællesoffentligt og internationalt kan give anledning til udfordringer i forhold til vedligeholdelse af standarder, hvis de ikke tydeligt adresseres. Det bør eksempelvis beskrives, hvordan lovbaseret (sub)profilering forholder sig til fællesoffentlige aftalebaserede profiler i tilfælde af revisioner på et af niveauerne. Reviewboardet finder, at der bør sikres formaliseret tilbageløb begge veje, som blandt andet kan håndtere ønsker og krav mm.

3. Det anbefales, at projektet forholder sig til kommunikation om gevinster.

Det er reviewboardets opfattelse, at der til understøttelse af implementering og forankring af nye standarder er behov for fokus på kommunikation om gevinster til anvendere og beslutningstagere. Reviewboardet anbefaler, at projektet adresserer dette.

4. Det anbefales, at projektet tydeliggør sammenhæng mellem arkitekturvalg og økonomi, sikkerhed, driftsstabilitet, effektivitet mv.

Arkitekturvalg, fx i forhold til tokens afgrænsninger og antal transaktioner, indebærer ofte en række konsekvenser på forskellige parametre. Det er reviewboardets anbefaling, at projektet bør tydeliggøre disse konsekvenser for at informere beslutningsgrundlaget for de konkrete valg. I tilfælde af at der er behov for at afveje fx sikkerhed vs. effektivitet eller økonomi vs. driftsstabilitet, er det nødvendigt, at konsekvenser af arkitekturvalg er tydelige.

5. Det anbefales, at projektet forholder sig til logningsbehov og krav afledt af databeskyttelsesforordningen.

Reviewboardet finder, at projektet bør afklare, hvorvidt der som følge af databeskyttelsesforordningen stilles krav, som projektet skal tage højde for, fx de registreredes rettigheder og i forhold til samtykke. Dette er ikke tydeliggjort i forbindelse med reviewet, ligesom logningsbehov ikke forekommer afklaret.