Initiativ 8.1
Handlingsplan for: 7.2 Afprøvning af fælles standarder for sikker information

Indholdsfortegnelse

Bemærkninger til indstilling fra review-rapport

Projektet er enige i reviewboardets overordnede indstilling, som er:

"Det er reviewboardets opfattelse at retning og scope som udlagt i det fremsendte materiale stem-mer godt overens med den vision og de principper, som hvidbog om fælles-offentlig digital arkitektur udtrykker.".

Handlingsplan for anbefalinger til projektet

Nedenfor følger projektets handlingsplan baseret på de anbefalinger, som følger af arkitekturreviewet, sammenfattet i den fremsendte reviewrapport. Det understreges, at nærværende handlingsplan og angivne konsekvenser for scope, tid og økonomi er projektets estimat, godkendt af projektejer, men endnu ikke behandlet i projektets styregruppe.

Anbefalinger

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

Anbefaling:

"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. "

Besvarelse:

Projektet er enige i anbefalingens relevans. Projektet mener, at anbefalingens indhold allerede er afklaret og omfattet af projektets planer.

På Sundhedsdatastyrelsens hjemmeside[1] beskrives rammerne for indførelse (og udbredelse) af IT-standarder indenfor sundhedsområdet, og projektet er omfattet af disse rammer:

"Fastsættelsen af rammer for it-arkitekturen og for de standarder der skal anvendes, sker i samarbejde med sundhedsvæsenets parter og Sundhedsdatastyrelsen. Alle standarder forelægges Det rådgivende udvalg for standarder og arkitektur[2], inden de endeligt godkendes og optages i standardkataloget.

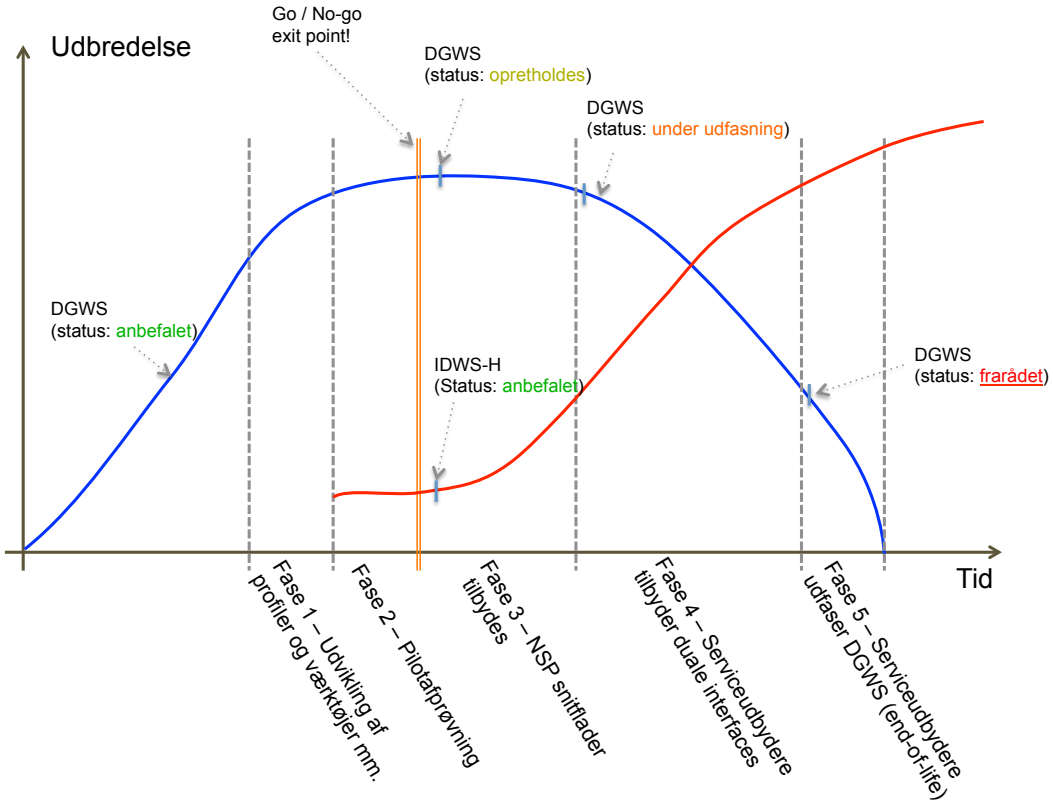
[1] https://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-referencearkitektur-og-standarder

[2] https://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-referencearkitektur-og-standarder/udvalg

Sundhedsdatastyrelsens arbejde med fastsættelse af forpligtende anbefalingsgrader er forankret i Bekendtgørelse nr. 160 (1. marts 2013) om standarder for it-anvendelse i sundhedsvæsenet.[3]"

I projektets PID fremgår, at IDWS/XUA sundhedsprofilen skal forelægges Det Rådgivende Udvalg for Standarder og Arkitektur på sundhedsområdet (RUSA) med henblik på godkendelse som national standard og optagelse i katalog over standarder på sundhedsområdet. Projektet planlægger en første behandling i RUSA i foråret 2018 med ønske om at sundhedsprofilen optages i kataloget med anbefalingsgrad "planlagt".

Den videre behandling i RUSA med oplæg til mere forpligtende anbefalingsgrad afhænger af en drøftelse i den nationale bestyrelse for sundheds-it i foråret 2019. I projektets sidste fase udarbejdes forslag til migreringsstrategi/-plan til behandling i bestyrelsen. Oplæg til migreringsplan vil formodentlig tage udgangspunkt i den skitse til migrering, som blev beskrevet i den tidligere gennemførte analyse af sikkerhedsstandarder[4]:



[3] https://www.retsinformation.dk/Forms/R0710.aspx?id=145514

[4] Den nye profil på sundhedsområdet betegnes her IDWS-H.
DGWS betegner Den Gode Webservice.

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

Anbefaling:
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.

Besvarelse:
Projektet er enige i anbefalingens relevans. Projektet mener, at anbefalingens indhold allerede er omfattet af projektets planer.

I projektet PID fremgår, at der i sidste fase af projektet skal udarbejdes en samlet governance-model for standarder og værktøjer. Governance-modellen skal dække såvel DIGST produkter som SDS produkter, samt deres påvirkning fra de internationale standarder der benyttes.

Sundhedsområdets profil baseres på den fælles offentlige OIO IDWS standard. DIGST har op til projekt start revideret IDWS, så den kan rumme de tilføjelser som sundhedsområdet har behov for (resultatet var OIO IDWS version 1.1). DIGST har desuden deltaget i den arbejdsgruppe, der har udarbejdet sundhedsprofilen, for at sikre profilens overholdelse af rammerne for IDWS standarden.

Sundhedsområdets profil tænkes understøttet af de samme værktøjer som stilles til rådighed af DIGST til udvikling af OIO IDWS webservices. Projektet finansierer tilføjelser til disse, der skal benyttes ved udvikling af webservices baseret på den sundhedsspecifikke profil, men disse vil blive en del af den samlede kodebase for værktøjerne, og ejerskabet til hjælpeværktøjerne tænkes fastholdt i DIGST.

Med fare for at foregribe arbejdet med governancemodel kan der skitseres følgende:

OIO IDWS ejes, vedligeholdes og supporteres af DIGST. Såfremt, der sker ændringer i de internationale standarder, som OIO IDWS baseres på, er det DIGST's ansvar at påvirke disse ændringer og/eller (i samarbejde med brugerne af OIO IDWS) at specificere ændringer til OIO IDWS, der sikrer fortsat overholdelse af internationale standarder. Der bør etableres fora (f.eks. Change Advisory Board) og processer, der inddrager brugerne i specifikation og diskussion af ændringer.

Den sundhedsspecifikke profil tænkes ejet af en part på sundhedsområdet (f.eks. Sundhedsdatastyrelsen eller MedCom) og underlægges den eksisterende governance for fastlæggelse af standarder på sundhedsområdet[5]. Såfremt, der sker ændringer i de interna-

[5] https://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-referencearkitektur-og-standarder

tionale sundhedsspecifikke standarder, som profilen baseres på, er det profilejerens ansvar at påvirke disse ændringer og/eller (i samarbejde med profilens brugere) at specificere ændringer til profilen, der sikrer fortsat overholdelse af internationale standarder. Hvis foreslåede ændringer kræver ændringer i OIO IDWS for at kunne realiseres, er det profilejerens ansvar, at der anmodes om ændringer (Request for Change) heraf i overensstemmelse med den governance (change-proces) der fastlægges for OIO IDWS, forud for eventuelle beslutning om ændring af sundhedsprofilen.

Ejeren af OIO IDWS (DIGST) og ejeren af sundhedsprofilen bør fastlægge hvilken support der ydes i forbindelse med vejledning af den respektive standard/profils anvendelse.

Hjælpeværktøjer (inklusiv sundhedsspecifik kode) ejes af DIGST og vedligeholdes og supporteres af leverandør efter aftale med DIGST. Der er også her behov for, at der etableres fora og processer, der sikrer parternes inddragelse i fremtidige ændringer. Der bør tages stilling til, hvilken leverandørsupport der ydes i forbindelse med anvendelse af værktøjer.

Ændring af infrastrukturkomponenter på sundhedsområdet, så disse tilpasses ny profil følger eksisterende governance for den nationale serviceplatform på sundhedsområdet (NSP). Dette er en del af det fællesoffentlige systemforvaltningskoncept på sundhedsområdet[6].

Projektets leverance vil konkretisere ovenstående.

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

Anbefaling:

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.

Besvarelse:

Projektet er enige i anbefalingens relevans.

Grundlaget for projektet er en analyse fra 2014 vedrørende gevinster og omkostninger ved at samordne sikkerhedsstandarder og sikkerhedsløsninger i sundhedsvæsenet med det øvrige fællesoffentlige samarbejde. Med udgangspunkt i konklusionerne fra analysen etablerede sundhedsområdets parter nærværende projekt. Dvs. formelt kender og anerkender regioner, kommuner og lægepraksissektoren de gevinster, som projektet skal realisere.

Undervejs i projektet er det dog erkendt, at den formelle anerkendelse af projektet gevinster ikke nødvendigvis er flydt ned til de enkelte organisationer og leverandører som

[6] Fællesoffentlig systemforvaltning af sundheds-it (FSI) blev etableret som led i økonomiaftalen for 2016 mellem Regeringen, KL og Danske Regioner.

skal realisere gevinsterne. Af denne grund vil det være værdifuldt at udarbejde et notat, der i kort form kan anvendes til at kommunikere de gevinster som projektet realiserer.

Dette notat udarbejdes i første kvartal af 2018 og forventes anvendt i den løbende kommunikation med projektets parter og interessenter.

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

Anbefaling:

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.

Besvarelse:

Projektet er enige i anbefalingens relevans.

I projektet vedligeholdes en arkitekturbeslutningslog, som lister de forskellige arkitekturvalg og begrundelserne for disse valg. Projektet vil uddybe denne beslutningslog med implikationer i forhold til sikkerhed, driftseffektivitet og –stabilitet, økonomi mm.

5. Det anbefales, at projektet forholder sig til logningsbehov og krav afledt af databeskyttelsesfor-ordningen.

Anbefaling:
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.

Besvarelse:
Projektet er enige i anbefalingens relevans, og planlægger foranlediget heraf en afklaring af, hvorvidt der som følge af databeskyttelsesforordningen stilles krav, som projektet skal tage højde for.

De krav som GDPR stiller til løsning udredes i Q1 2018. Den sikkerhedsansvarlige for Sundhedsministeriet og styrelserne kontaktes i den forbindelse. Listen af udredte krav anvendes efterfølgende i forbindelse med design og arkitekturvalg.

Opsummering på handlingsplan

Projektet er enige i alle anbefalingers relevans. Projektet vurderer, at anbefaling 1 og 2 allerede er omfattet af projektets eksisterende planer og derfor blot kræver yderligere konkretisering. Anbefaling 3, 4 og 5 resulterer i følgende nye aktiviteter:

1. **Notat med gevinstrealisering:** Der udarbejdes et notat, der kan anvendes til at kommunikere de gevinster som projektet realiserer. Dette notat udarbejdes i første kvartal af 2018 og forventes anvendt i den løbende kommunikation med projektets parter og interessenter.
2. **Uddybning af arkitekturbeslutningslog:** Der tilføjes afsnit, der beskriver implikationer i forhold til sikkerhed, driftseffektivitet og –stabilitet, økonomi m.m..
3. **Udredning af GDPR krav til løsningen**: De krav som GDPR stiller til løsning udredes i første kvartal af 2018. Den sikkerhedsansvarlig fra Sundhedsministeriet og styrelserne kontaktes i den forbindelse. Listen af udredte krav anvendes efterfølgende i forbindelse med design og arkitekturvalg.

De to aktiviteter estimeres til ca. 125 konsulent timer og forventes afviklet indenfor projektets eksisterende økonomi.