Digitaliseringsstyrelsen
Kontor for data og arkitetur

Reviewrapport for:
Brugerstyring i Danmarks Miljøportal

Indhold

Review af brugerstyring i Danmarks miljøportal

Arkitekturreviewet af brugerstyring i Danmarks Miljøportal (DMP) er udført på baggrund af projektets fremsendte materialer: Dokumentationsramme for Danmarks Miljøportals brugerstyring, Usecase login, VSTS backlog items.xlsx, Token for login – eksempel, Målarkitektur for Danmarks Miljøportal, PID brugerstyringsopgradering, Præsentation til arkitektur review 23 oktober, GHlobeteam oplæg DMP IT arkitektur, Use cases brugerstyring opgradering, Scenarier for brug af DMPs brugerstyring, Roller og flows i brugerstyring, Tilsluttede systemer til DMPs brugerstyring.

Reviewet er ikke gennemført i regi af FODS initiativ 8.1, men på forespørgsel fra DMP. Dette er i tråd med hvidbog om fællesoffentlig digital arkitektur, hvori det fremgår, at den fællesoffentlige arkitektur i projekter uden for FODS ligeledes kan være hensigtsmæssig at anvende. Selve reviewprocessen er udført i overensstemmelse med rammerne i den fællesoffentlige arkitektur, herunder model for reviews, godkendt af styregruppen for data og arkitektur maj 2017. Dog bemærkes det, at reviewet er udført alene af sekretariatet for initiativ 8.1/kontor for data og arkitektur i regi af Digitaliseringsstyrelsen med ekstern observatør fra Miljøstyrelsen:

Ekstern observatør:	Thomas Hjorth Rasmussen, Miljøstyrelsen
Sekretariat for 8.1 /Kontor for data og arkitektur, Digitaliseringsstyrelsen:	Sarah Kirkeby Danneskiold-Samsøe, sek.
	Mads Hjort, arkitekt
	Kirsten Taarnskov, sek.
	Lars Thomsen, arkitekt
Projektdeltagere:	Nils Høgsted, DMP
	Michael Buch-Larsen, DMP
	Jesper Nørmark, DMP
	Martin Strandbygaard, Globeteam

Reviewgrundlag

Udgangspunktet for reviewet udgøres af referencearkitektur for brugerstyring og hvidbog om fællesoffentlig digital arkitektur, herunder hvidbogens principper og regler for arkitektur godkendt i styregruppen for data og arkitektur maj 2017. Hvidbogens principper og relevante principper fra referencearkitektur for brugerstyring er gengivet nedenfor.

1. *Arkitektur styres på rette niveau efter fælles rammer (styring)*
    a. Brugerstyring: Princippet om sammenhængende adgangsstyring for brugere bør efterkommes
2. *Arkitektur fremmer sammenhæng, innovation og effektivitet (strategi)*
    a. Brugerstyring: Princippet om føderationer baseret på tillid og aftaler bør efterkommes
    b. Brugerstyring: Princippet om brugerstyring i overensstemmelse med internationale standarder
3. *Arkitektur og regulering understøtter hinanden (jura)*
    a. Brugerstyring: Princippet om styring af informationssikkerhed i føderationer er en følge af ISO/IEC 27001, ISO/IEC 27005, EU's General Data Protection Regulation (GDPR) og den danske persondatalov og skal efterkommes

   b. Brugerstyring: Dansk Standard DS 844 er en alternativ standard for navngivning af certifikater. Denne skal forlades i nye løsninger
4. *Sikkerhed, privatliv og tillid sikres (sikkerhed)*
   a. Brugerstyring: Princippet om respekt for brugernes privatliv skal efterkommes
5. *Processer optimeres på tværs (opgaver)*
   a. Brugerstyring: Princippet om tjenesteudbyderes håndhævelse af brugeres adgang er en følge af krav i Persondataloven om dataansvar, og derfor skal det efterkommes af alle med dataansvar
   b. Brugerstyring: Princippet om fokus på brugernes behov bør efterkommes
   c. Brugerstyring: Princippet om administration af brugere udenfor fagapplikationer bør efterkommes
   d. Brugerstyring: Den tekniske opbygning af brugerstyringmed opdeling i klart adskilte delprocesser og arbejdsdeling mellem aktørerne i administrative processer og autentifikation, billetudstedelse og adgangskontrol samt kontrol og rapportering bør efterkommes
6. *Gode data deles og genbruges (information)*
   a. Brugerstyring: Begrebsmodellen kan anvendes i løsninger, der kommunikerer mellem offentlige sektorer, og i tjenester, der anvender fællesoffentlige løsninger
   b. Brugerstyring: Brugerstyringstjenester og forretningstjenester i fællesoffentlige føderationer, der anvender attributter, skal vurdere om kvaliteten af attributter svarer til tjenestens behov
   c. Brugerstyring: Identitetsbrokere bør kommunikere sikringsniveauet for autentifikationen ved at indlejre en attribut i billetten, som angiver dette
7. *It-løsninger samarbejder effektivt (applikation)*
   a. Princippet om løst koblede brugerstyringskomponenter bør efterkommes
   b. Princippet om brugerstyring baseret på fælles kerne i samspil med øvrige komponenter skal efterkommes
   c. OIOSAML og OIO Basic Privilege Profile har status af anbefalede fællesoffentlige standarder og bør som minimum følges, når der er behov for håndtering af eksterne brugere i web applikationer
   d. Opbygning af brugerstyring med byggeblokkene Registrering af elektronisk identitet, Akkreditivtilknyting, Attributbeskrivelse, Autentifikation, Billetudstedelse og adgangskontrol bør efterkommes
8. *Data og services leveres driftssikkert (infrastruktur)*
   a. Arkitektur med identitetsbrokere bør efterkommes
   b. Understøttelse af notificerede eID-løsninger fra andre EU-lande bør ske gennem national eID gateway, der stilles til rådighed af Digitaliseringsstyrelsen
   c. Standarden OpenID Connectkan på kort til mellemlang sigt tilbydes som et supplement til SAML 2.0 services

Projektresume

Reviewet foretages i forbindelse med et opgraderingsprojekt af DMP's brugerstyring, som udover DMP anvendes af ca. 20 andre systemer hos andre organisationer herunder KOMBIT, GeoDanmark, Miljøstyrelsen og Søfartsstyrelsen. DMP's brugerstyring giver adgang til fagsystemer med data, der stilles til rådighed af offentlige virksomheder. Arbejdet med den fremtidige brugerstyring har til formål at sikre, at adgang til data håndteres sikkert både for interne og eksterne data, at omkostninger til drift og support bliver mindre samt at brugerne vil opleve bedre performance og øget brugervenlighed.

Indstilling

Det er vurderingen på baggrund af reviewet, at DMP's brugerstyring er i overensstemmelse med principper og regler herfor i den fællesoffentlige arkitektur, med fokus på referencearkitektur for brugerstyring samt hvidbog om fællesoffentlig digital arkitektur.

7 ud af 8 af hvidbogens principper vurderes i grøn. Det bemærkes positivt, at DMP i deres tilgang til platforms- og applikationservices er eksplicit opmærksomme på rettigheder og ejerskab til den integrationskode, der binder de forskellige dele af løsningen sammen. Dette understøtter anvendelse af standardkomponenter samtidig med, at det letter et eventuelt leverandørskifte på et senere tidspunkt og er derved bidragende til niveauet af dataportabilitet og følgende fremtidssikring af løsningen.

Perspektivet om infrastruktur vurderes som værende gult, dvs. i delvis overensstemmelse med hvidbogens princip og referencearkitektur for brugerstyring på dette område. Dette funderes i særdeleshed i referencearkitekturens regel om, at fællesoffentlige løsninger bør basere deres løsninger på en fælles kerne. Her er det opfattelsen fra reviewet, at der i DMP projektet ikke eksplicit er taget stilling til, hvad der udgør en eventuel fælles kerne. Det bør eksplicit overvejes hvilken rolle den fællesoffentlige brugerrettighedsstyring (FBRS) skal have i den forbindelse.

Anbefalingerne givet i review-rapporten er udtryk for, hvad der på baggrund af reviewet vurderes som væsentligt, at DMP forholder sig til i det videre projekt.

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

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

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

Hertil er udarbejdet **2** tværgående anbefalinger, hvortil sekretariatet laver beslutningsoplæg til styregruppen for data og arkitektur.

Anbefalinger

Reviewet af DMP's brugerstyring har identificeret en række anbefalinger, der fremstår i to kategorier:

1. Anbefalinger til det nuværende projekt: Herunder fremstår anbefalinger til projektet i dets nuværende og kommende faser.
2. Tværgående anbefalinger: Disse anbefalinger identificeres i reviewet som centrale og relevante for projektets fremtidige succes, men samtidig af en sådan karakter, at disse udfordringer ikke kan løses af projektet isoleret set.

For så vidt angår anbefalinger i kategori 1, anmodes projektet om at imødegå disse ud fra følg-eller-forklar princippet i deres bemærkninger til review-rapporten samlet i en handlingsplan. For anbefalinger i kategori 2, inddrager sekretariatet anbefalinger i det videre arbejde i regi af FODS initiativ 8.1.

Anbefalinger til det nuværende projekt

1. Det anbefales, at DMP inddrager relevante parter i en drøftelse af, hvad en fælles kerne er, samt hvilket omfang og hvilken anvendelse den har.

Referencearkitekturen kan danne udgangspunkt for drøftelsen. En kerne kan både være genanvendelse af fælles applikationskomponenter, data eller etablering af fælles proces-beskrivelser. Kandididaterne til fælles elementer kunne være attributlister, aftale-skabeloner og vejledning i opfyldelse af asssurence-levels.

2. Det anbefales, at DMP afklarer, hvilken rolle FBRS spiller i forhold til rettighedsstyring for myndigheder og virksomheder.

Særligt små- og mellemstore vil forvente at kunne se et komplet overblik over hvilke roller de har tildelt til deres medarbejdere. Roller tildelt i DMPs brugerstyring kunne måske kopieres til FBRS som 'read-only'.

3. Det anbefales, at tjenesteudbydere i DMP - i forbindelse med revurdering af adgangspolitikker - overvejer hvor eksplicitte roller kan erstattes af allerede registrede attributer.

Adgangspolitikker bør også vurderes i forhold til hvor effektivt de kan implementeres, både hos tjenesteudbyder, infrastruktur og hos brugerorganisationer.

4. Det anbefales, at DMP inddrager de igangværende aktiviteter i digitaliseringsstrategiens initiativ 7.3 i overvejelserne om valg af gateway mod europæiske eID løsninger.

DIGST er i gang med et udbud omkring en national gateway til brug for udenlandske eID løsninger. Projektet kan kontaktes via hjemmeside.

5. Det anbefales, at DMP anvender referencearkitekturens begreber.

Særligt er begreber som godkendelse, genkendelse, adgangspolitik og sikringsniveau centrale for at tjenesteudbydere kan sammenligne brugerstyringsløsninger.

6. Det anbefales, at DMP refererer til referencearkitekturens byggeblokke.

Forretnings- og applikationsroller bør knyttes på de produkter og komponenter som - i DMPs arkitektur - udfylder rollerne. KDA kan hjælpe med eksempler og vejledning.

7. Det anbefales, at DMP som identitetsbroker overvejer om man vil tilbyde forskellige niveauer af sikkerhed (insurance levels).

Sikkerhed i forbindelse med brugerstyring bliver kun vigtigere i sammenhængende og offentlige it-løsninger. I forhold til DMP løsningen er der overvejelser på, hvilken sikkerhed og hvilke sikkerhedsniveauer man kan tilbyde samlet set - når der er tale om føderationer af brugerstyring. Det bør derfor overvejes, hvordan man vil håndtere denne problematik ift. garanti for sikkerhedsniveauer, og hvis man vælger at tilbyde forskellige levels, overvejes det desuden, hvordan dette gøres.

8. Det anbefales, at arkitekturen for DMPs brugerstyring indeholder identifikation af de nødvendige brugeradministrationsaftaler i føderation.

Det er særligt vigtigt at DMPs tjenesteudbydere kan understøttes i vurderingen af, hvordan sikringsniveauer implementeres hos de fødererede identitetsudbydere.

Tværgående anbefalinger

9. Det anbefales, at føderationer, der indgår i brugerstyringen, identificeres, samt at der defineres minimumskrav til dem ift. det sikringsniveau (trust / insurance lvl), der tilbydes. Kravene bør kobles med insurance levels, der fremgår af NSIS og NIST.

For at styrke overblik og administration af tværgående brugeradministrationsaftaler bør der stilles ensartede minimumskrav til de systemer, der fødereres ind i brugerstyringsløsningen.

10. Det anbefales, at governancestruktur for domæneanvendelse af fællesoffentlig brugerstyring afklares.

Der ligger en stor implementeringsopgave og værditilførsel ved, at fællesoffentlig brugerstyring tilpasses domænespecifikke forhold og tages i anvendelse. En fællesoffentlig brugerstyring har et stort potentiale ift. en domænespecifik anvendelse. Derfor er det også en anbefaling, at det afklares, hvordan de domænespecifikke "profileringer" af en fællesoffentlig brugerstyring kan spille tilbage på den generelle brugerstyring. Herved kan domænerne bidrage til en revision og forbedring - og dermed et større anvendelsespotentiale for den fællesoffentlige brugerstyring.