# ***Udvalget for arkitektur og data***

# **Reviewrapport for: Referencearkitektur for brugerstyring version 1.1**

20. april 2020

**Indhold**

[***Udvalget for arkitektur og data*** 1](#_Toc38551203)

[**Reviewrapport for: Referencearkitektur for brugerstyring version 1.1** 1](#_Toc38551204)

[Referencearkitektur for brugerstyring 1.1 2](#_Toc38551205)

[Projektresume 2](#_Toc38551206)

[Anbefalinger 2](#_Toc38551207)

[Anbefalinger til de nuværende projekter 3](#_Toc38551208)

[Tværgående Anbefalinger 4](#_Toc38551209)

# Referencearkitektur for brugerstyring 1.1

Reviewet af referencearkitektur for brugerstyring er udført 17.-27. april 2020 på baggrund af projektets fremsendte materialer:

1. Referencearkitektur for brugerstyring 2020 04 08.docx

Reviewet er udført i overensstemmelse med retningslinjer for arkitekturreviews, godkendt af styregruppen for data og arkitektur maj 2017. Særligt for dette review blev workshoppen foretaget virtuelt, grundet COVID-19 restriktioner på at mødes fysisk. Sekretariatet takker alle deltagere for fleksibiliteten.

Udgangspunktet for reviewet udgøres af hvidbog om fællesoffentlig digital arkitektur. Det er i bilag 1 udarbejdet en kortlægning af hvilke arkitekturregler der har motiveret de givne anbefalinger til projektet, og som med fordel kan læses for at understøtte overensstemmelse med hvidbogens principper. Reviewboardet og deltagere er listet i nedenstående tabel:

|  |  |  |
| --- | --- | --- |
| **Reviewboard:** | Kim Newton Kassebeer, Arkitekt | Styrelsen for dataforsyning og effektivitet |
|  | Lars Simesen, Arkitekt | Region midt |
| **Sekretariat for 8.1:** | Sven Rostgaard Rasmussen, Arkitekt | Digitaliseringsstyrelsen - CTD |
|  | Asbjørn Flyger Lauwersen, Facilitator | Digitaliseringsstyrelsen - CTD |
| **Projektdeltagere:** | Kirsten Taarnskov, Projektleder | Digitaliseringsstyrelsen |
|  | Thomas Gundel, Arkitekt | IT Crew |

# Projektresume

Formålet med referencearkitektur for brugerstyring er at målrette og strukturere brugerstyringen i det offentlige for at skabe sammenhængende, effektive, sikre og brugervenlige løsninger på tværs af domæner, nationalt og transnationalt.

Foruden brugerstyring af personer beskriver den opdatering af referencearkitekturen som her er reviewet også hvordan, referencearkitekturens principper for brugerstyring anvendes ved håndtering af softwarerobotter som separate identiteter med egne identifikationsmidler. Tilsvarende er referencearkitekturen udvidet med beskrivelser af, hvordan principperne kan anvendes ved brugerstyring af apps og apparater (IoT).

Brugerstyring defineres i denne arkitektur som administration og kontrol af brugere, identifikationsmidler og adgang til forretningstjenester. Det sikres, at de rette brugere får adgang til de rette it-systemer og data, og at alle andre afvises. Dermed berører referencearkitekturen en væsentlig del af den samlede informationssikkerhedsindsats i det fællesoffentlige samarbejde.

Reviewboardet vil gerne kvittere for det gode arbejde der er lagt i opdateringen, og den høje kvalitet det har resulteret i.

# Anbefalinger

Reviewet af *referencearkitektur for 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, som det er præsenteret for reviewboardet.
2. Tværgående anbefalinger: Disse anbefalinger identificeres af reviewboardet som centrale og relevante for projektets fremtidige succes, men samtidig af en sådan karakter, at disse udfordringer ikke kan løses af projektet isoleret set.

Anbefalingerne til det nuværende projekt anmodes projekterne om at imødekomme ud fra følg-eller-forklar princippet i deres bemærkninger til reviewrapporten samlet i en handlingsplan.

For tværgående anbefalinger, udarbejder sekretariatet for initiativ 8.1 beslutningsoplæg, som ligeledes indgår ligeledes i udvalget for arkitektur og datas behandling af reviewet.

## Anbefalinger til de nuværende projekter

**1. Det anbefales, at projektet udvider værdiafsnittet, med fokus på hvordan enighed om at anvende åbne og internationale standarder understøtter en god konkurrence i udbudssituationer.**

Anbefalingen er motiveret af arkitekturreglerne *AR 2.2 – Anvend åbne og internationale standarder* og *AR 2.3 – Undgå afhængighed af leverandører og proprietære teknologier.*

Når man kan læne sig op af en stabil gruppe udpegede standarder i udbud over længere tid giver det markedet mulighed for at prioritere at lære at anvende disse standarder, hvis de ikke allerede kender til dem. Dette giver et større udvalg af leveringsdygtige leverandører og understøtter dermed en sund konkurrence i udbud af offentlige it-løsninger. Det er vigtig gevinst ved at fælge referencearkitekturen, og bør indgå i værdiafsnittet.

**2. Det anbefales at projektet udvider juraafsnittet med betragtninger om kommende relevante retningslinjer og forordninger fra EU, eksempelvis den kommende eIDAS opdatering og SDG forordningen.**

Anbefalingen er motiveret af arkitekturreglerne *AR 1.1 – Styr arkitekturen på rette niveauer og sammenhængende* og *AR 3.1 – Tag højde for juridiske bindinger i forhold til deling og genbrug af data og it-systemer*.

Offentlig digital brugerstyring strækker sig i højere og højere grad ud over de nationale grænser, og spreder sig til EU's indre marked. Det er derfor relevant at have en forståelse for hvilke retningslinjer og forordninger der former den europæiske brugerstyring nu og i nærmeste fremtid. Derfor bør den kommende opdatering af eIDAS forordningen og SDG forordningen behandles i jurakapitlet i referencearkitekturen.

**3. Det anbefales, at Sikkerhedsafsnittet skærpes, så læseren ikke risikere at tolke retningslinjerne fra ISO 27001, som et opdrag til at lave proprietære sikkerhedsløsninger, men blot lokale risikovurderinger.**

Anbefalingen er motiveret af arkitekturreglerne *AR 2.3 – Undgå afhængighed af leverandører og proprietære teknologier* og *AR 2.4 – Byg med udgangspunkt i brugeren og forberedt til forandring*.

Anbefalingen tager udgangspunkt i følgende sætning fra sikkerhedsafsnittet i referencearkitekturen:

*Organisationens ledelse fastlægger på baggrund af en risikovurdering et sikkerhedsniveau, som svarer til den forretningsmæssige betydning af de aktiver (fx informationer), som organisationen ejer, vedligeholder og har dataansvaret for, og de tjenester som den stiller til rådighed for andre organisationer af alle typer.*

Ovenstående sætning kan misforstås, som at lokale risikovurderinger som ISO 27001 foreskriver, åbner op for at ledelsen i offentlige myndigheder udelukkende skal tage højde for risikovurderingen når informationssikkerheden skal fastsættes for myndigheden. Der er ikke tilfældet og bør tydeliggøres.

**4. Det anbefales, at der for at understøtte læsevenligheden laves flere referencer internt i dokumentet, det hjælper læseren med at navigere i dokumentets struktur.**

Anbefalingen er motiveret af arkitekturreglen *AR 2.4 – Byg med udgangspunkt i brugeren og forberedt til forandring.*

Generelt set er dokumentets struktur, der følger hvidbogens perspektiver til at finde rundt i. Dog kan en læser der ikke har en intuitiv forståelse for hvidbogens struktur sidde tilbage med spørgsmål der bliver besvaret grundigt andre steder i dokumentet. Projektet bør derfor anvende interne henvisninger hvor det giver mening, og i højere grad end nu.

**5. Det anbefales at referencearkitekturen nævner de mest relevante eksisterende og kommende tekniske standarder for brugerstyring på EU-niveau, som man bør være opmærksom på når man skal lave grænseoverskridende brugerstyring i EU, under informationsafsnittet.**

Anbefalingen er motiveret af arkitekturreglerne *AR 1.1 – Styr arkitekturen på rette niveauer og sammenhængende* og *AR 2.2 – Anvend åbne og internationale standarder.*

For at understøtte en lettere understøtte en dansk ensartet og korrekt tilgang til brugerstyring på EU-niveau bør de tekniske standarder der anvendes til brugerstyring på Europæisk niveau behandles i referencearkitekturens informationsafsnit.

**6. Det anbefales, at listen over brugerstyringsløsninger bør introduceres yderligere, samt at ejerne af de udvalgte løsninger kontaktes med henblik på at få kvalificeret listens indhold.**

Anbefalingen er motiveret af arkitekturreglerne *AR 2.1 anvend og udbyg den fælles arkitektur* og *AR 2.4 – Byg med udgangspunkt i brugeren og forberedt til forandring.*

Det kan være svært for en læser at gennemskue formålet med listen over løsninger i slutningen af infrastrukturafsnittet, og dette kan fører til misforståelser. Introduktionen bør derfor uddybes, og beskrivelsen af de enkelte systemer bør godkendes og/eller uddybes af systemejerne, så de med sikkerhed stemmer overens med virkeligheden og formålet.

## Tværgående Anbefalinger

**1. Det anbefales, at FDA etablere et arbejdsflow for centrale dokumenter med en løbende udstilling af forandringer, kommende releases, alfa versioner og gældende versioner, så det er muligt at lave hurtige ændringer når det kræves, at orientere sig i kommende forandringer løbende og at tage i mod bidrag.**

Anbefalingen er motiveret af arkitekturreglerne *AR 1.2 – optimer arkitektur efter projektets og de fælles mål* og *AR 2.4 – Byg med udgangspunkt i brugeren og forberedt til forandring.*

For at anvenderne af FDA løbende kan følge udviklingen af arkitekturen, indmelde nye behov og dele egne erfaringer igennem den fælles arkitektur, kan det være gavnligt at åbne mere op for den løbende udvikling af centrale FDA-dokumenter. Det kan inkludere en tydelige release rækkefølge, og en mulighed for at komme med forslag til direkte tekstforandringer eller tekstnære kommentarer.