DIGITALISERINGSSTYRELSEN

Kommenteringsskema

15. januar 2018
Sekretariatet for
Initiativ 8.1.

BEMÆRK: Alle indsendte kommentarer offentliggøres (på arkitektur.digst.dk). Såfremt du *ikke* ønsker en kommentar offentliggjort, bedes du gøre opmærksom på det i mailen.

Den udfyldte skabelon sendes til arkitektur@digst.dk.

Dokumentet/dokumenter der kommenteres på:

1. **faelles_retningslinjer_for_webservices_v0.9.docx**
2. **bilag_1_digst_dokumentation_for_rest_webservices**
3. **bilag_2_fejlstruktur_og_fejlkoder_for_rest_webservices**
4. **bilag_3_nonfunktionelle_krav_til_realisering_af_retningslinjer**
5. **bilag_4_specifikation_for_brug_af_http_til_rest**

Organisationen der kommenterer: Sundhedsdatastyrelsen

Kontaktperson for evt. uddybelse: Henrik Buch-Larsen

Kommentarer:

Generelt:

Det ville være ønskværdigt at der var en mere tydelig sammenhæng mellem de Strategiske mål for arbejdet og hvilke service design principper der understøtter disse mål, endvidere en kobling til de konkrete anbefalinger som understøtter de enkelte principper. Se f.eks. "Principles of Service Design" af Thomas Earl.

Hvem er målgruppen for disse dokumenter. Hvilke forudsætninger skal læseren have?

Der mangler generelt en beskrivelse af de sikkerhedsmæssige principper og protokoller svarende til IDWS funktionalitet for REST baseret kommunikation.

ad 1)

Side 8-10: Temaerne virker lidt som tilfældige nedslagspunkter med forskellige dybde.

F1 er eksempelvis en blanding af noget meget generelt "omkostningseffektivt i et fællesoffentligt perspektiv" og et meget konkret krav til værktøjsunderstøttelse ved serviceudvikling.

F2: "Design af webservices skal tage udgangspunkt i serviceanvenderens behov." Hvilke behov? Der er mange interessenter i forhold til design af webservice. Det virker for snævert at fokusere på service anvender.

F3 beskriver ændringer i webservices. Hvorfor ikke først beskrive principper for design af services så ændringsbehovet minimeres?

F4 er relateret til design af forretningsprocesser hvilket ikke giver meget mening i forhold til webservicedesign

I løbet af disse fire krav berøres så forskellige temaer som etableringsomkostninger, værktøjsunderstøttelse, interessenter, ændringshåndtering og forretningsprocesser uden specielt megen sammenhæng. Denne stil fortsætter gennem resten af kravene - det fører for vidt at gå gennem dem alle her.

Der er behov for en grundig restrukturering af temaerne så de hænger bedre sammen.

Side 10-13: Rigtig mange ord. Mange af disse beskrivelser minder om de fire grundlæggende service principper, men det er uklart om det er udgangspunktet:

1. Boundaries are explicit
2. Services are autonomous
3. Services share Schema and contract, not class
4. Service compatibility is based on polices

Vi er af den opfattelse, at man ikke kan give anbefalinger i forhold til opdeling i services og operationer (granularitet) uafhængig af den kontekst hvori servicene skal virke (forretningsmæssigt og teknologisk). Tilsvarende vil spørgsmålet om hvor målrettede eller hvor generiske services skal være, helt afhænge af hvilken rolle servicen spiller i arkitekturen (f.eks. om den er tæt på GUI eller den er en støtteservice for andre services). Man kan ikke slutte, at generiske services nødvendigvis gør en løsning mindre forandringsparat. Det modsatte kan også være tilfældet. Vi finder derfor ikke teksten før regel R01 og selve reglen særlig gyldig.

Side 14: Krav til forretningsprocesser bør løftes ud af dette dokument.

Side 17: Krav til service opmærkning og metadata. Det virker som et tilfældigt nedslagspunkt i et meget stort område omkring datamodellering og

begrebsstandarder. Det hører nok under krav til kontrakter og metadata, herunder service discovery.

Side 18: Krav til fejlkoder. Det virker besynderligt at fokusere på fejlkoder uden at starte med en overordnet beskrivelse af retningslinier for kontrakt og skema.

Det er heller ikke altid muligt at beskrive fejlkoder, da de kan være eskaleret fra bagvedliggende systemer.

Side 19: Versionering af webservices. Hvorfor ikke lave en fællesoffentlig profil for webservice metadata og registrering, i stedet for disse overordnede anbefalinger.

Side 22: Er der tale om audit eller SLA log. Hvorfor ikke stille krav om beskrivelse af hvilke data der logges?

Side 27: Temporale ressourcer. Afsnittet fremhæver dette område ud af mange forhold omkring den forretningsmæssige side af service design. Enten bør det fjernes eller også bør beskrivelserne udvides med en række andre områder som hører til emnet service design.

Side 33: Sikkerhedskrav til webservice. Afsnittet er ikke fyldestgørende for beskrivelse af sikkerhed for webservices. Giv gerne interessenterne nogle guide lines for hvordan de kan klassificere en service sikkerhedsmæssigt og henvise til yderligere krav i profiler mv.

Side 35: Undlad lærebogsagtig information hvis ikke det er konsekvent og gennemført. Beskrivelsen af R24 implikationer er et eksempel på en lidt for pædagogisk skrivemåde. Henvis i stedet til standarder og artikler.

Side 35: R25: "REST webservices udstiller data som ressourcer". Her bør man overveje at definere ressourcer, ellers giver sætningen ikke megen mening for en læser der ikke kender REST. REST er en forkortelse for Representational State Transfer, så formelt er der tale om at servicen returnerer en repræsentation af en tilstand i et system. Ressource er et koncept. REST services returnerer en ressource-tilstand – ikke en ressource.

Igen – er der behov for at forklare principperne bag REST? Man risikerer at få skrevet noget der er upræcist eller i værste fald forkert.

Side 36: R26,27,28. Løft krav til datamodeller op på et generelt niveau for webservices. Kravene bør også gælde for SOAP webservices.

Side 30: Præciseres. Er der tale om fysiske referencer mellem tilstands repræsentationer (ressourcer) eller om de logiske relationer mellem entiteter?

Flyt teksten: ” REST arkitekturstilen fastlægger, at hypertext, dvs. indhold med aktive links der kan navigeres efter, er måden, hvorpå ressourcer tilgås. REST webservices bør derfor informere om sig selv og om relevante andre ressourcer via hypertext links.” til R30.

Der udestår en afklaring af infrastrukturen der skal binde disse ressourcer sammen på tværs af serviceudbydere. Fælles offentlig DNS arkitektur, kunne være en mulighed, sammen med navnestandarder for URL’er og forretningsgange for registrering og udstilling af nationale REST services (indeks). Dermed vil det være muligt at indlejre referencer til ressourcer uden for det lokale domæne.

Side 45: ”HTTP består af en request struktur og en response struktur.” Brug de korrekte begreber i hht. RFC 2616; HTTP Message (besked)

Side 45: ” Webservices bør returnere specifikke fejlkoder, hvis serviceanvenderen bruger usikker HTTP (dvs. uden kryptering og autentificering) i stedet for automatisk at omstille serviceanvenderen til en sikker HTTP. ”

Det bør være tilstrækkeligt at kunne udstille services gennem HTTPS. Det bør ikke være et krav at man kan svare på et HTTP kald ud over de standard fejl der returneres fra serveren såfremt der ikke påbegyndes en TLS forhandling fra klientens side.

Side 46: R39. ”De URI’er, der anvendes til ressourcer, bør ikke indeholde fortrolige eller følsomme data”. Det bør overvejes at udarbejde nogle anbefalinger til hvordan denne problemstilling kan håndteres. I lyset af hvor meget der gøres ud af, f.eks. temporaler, bør der også anvises principielle løsningsmodeller for dette område.

Side 47. R40. Man bør tage stilling til JSON Web Tokens (RFC7519) som løsningsmodel i forhold til sikkerhed.

ad 2)

Generelt:

- Fint at OpenAPI er grundlaget for metadatabeskrivelsen.
- Uhensigtsmæssigt at navne er på dansk - brug engelsk i stedet. Disse beskrivelser skal kunne læses af standardværktøjer.

ad 3)

Generelt

- Brug engelske feltnavne.

ad 4)

Generelt

- Der er tale om en lang række yderligere krav til services. De bør beskrives på samme måde som i 1). Kravene bør tilføjes til de fælles retningslinier og ikke kun være del af en tilbudsramme.

ad 5)

- Det virker risikabelt at man prøver at "forklare" hvordan HTTP protokollen skal anvendes. Om nødvendigt, bør der foretages en egentlig profilering (Fremhæv evt. KAN, SKAL, BØR osv.)