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: Fælles retningslinjer for webservices

Organisationen der kommenterer: SKAT - Løsningsarkitektur og Test

Kontaktperson for evt. uddybelse: Brian.Jakobsen@skat.dk

Kommentarer:

Sikkerhed i transportlaget

Afsnit 3.9 og 4.5: (Sikkerhedskrav til hhv. webservices og REST-webservices)

Der er skitseret anvendelse af sikkerhed i transportlaget, hvor besked-baseret sikkerhed med signatur på hver meddelelse havde været at foretrække, da det bl.a. giver mulighed for at opnå uafviselighed af transaktioner.

Ulemper ved skitserede retningslinjer:

Ingen uafviselighed: Det er ikke muligt at bevise at serviceaftager har udført en given transaktion.

Der er intet fysisk bevis (f.eks. en signatur) på at meddelelsen indeholdt det modtagne, hvormed der kan opstå tvister om hvad der var indeholdt i meddelelsen.

DIGST begrundelse for valg:

"Håndtering af punkt til punkt forbindelser, fx ved anvendelse af certifikater, er tungt at håndtere administrativt."

Har man ikke samme problematik med transportbaseret sikkerhed hvor service-aftager og -udstiller ønsker at autentificere sig op i mod hinanden?

Det havde været at foretrække der blev angivet retningslinjer for besked-baseret sikkerhed for at understøtte forretninger med dette behov.

Kapitel;Side	**Reference tekst (udsnit af tekst der kommenteres på)**	**Kommentar**
1;3	Det er væsentligt, at anvendelsen af retningslinjerne finder sted i samspil med eksisterende retningslinjer og standarder, således at der ikke skabes unødig kompleksitet. De fælles retningslinjer er særligt anvendelige, hvor der ikke foreligger domænespecifikke standarder og retningslinjer for webservices.	Vi forstår godt denne for domæner, men havde gerne set at man havde en målsætning om rummelighed i stedet
1.1;4	• Retningslinjerne stiller ikke krav om hvornår temporaler	Hvordan skal krav forstås i forhold til retningslinier?
1.1;4	• Retningslinjerne i dette dokument kan den enkelte organisation vælge at anvende inden for egen organisation for at skabe	Denne bemærkning bør hives med op i indledningen
1.1;4	men det er ikke et krav.	Dette er en tautologi: en retningslinie er ikke et krav
1.3;6	Opdateret	Opdelt
3;11	3. Generelle retningslinjer for webservices	Der ønskes en retningslinie der fokuserer på roller i snitfladen , for på denne måde at have et fælles grundlag for at specificere ansvar og pligter
3.1;12	genbrugeligheden af den enkelte webservice bliver reduceret.	har svært ved at se at dette reducerer genbrugelighed. Der er jo blot tale om at gøre services der udstille mere atomariske og lade det op til orkestreringen at komponere disse. Skriv og læs på samme service er således normaliseret tilstrækkeligt
3.1;13	Webservices skal designes, så snitfladen udstiller egne datasæt og ikke har eksterne afhængigheder til andre domæners objekter.	Retningslinien er ikke helt klart Er det for at undgå at et datasæt indeholder data fra eksterne låne-objekter??
3.1;13	Når webservicen udstiller en facade foran den bagvedliggende forretning, får serviceanvenderen kun det nødvendige data, for at reducere kompleksitet og gardere mod konsekvenser af ændringer fra bagvedliggende systemer	Ja det er vigtigt at anvenderen kun modtager hvad denne har brug for , hverken mere eller mindre Men jeg har svært ved at se 1:1 relevans til R03?
3.1;13	Forretningsmæssige webservices, der udstiller data, kan være en aggregering af data fra andre webservices	Ja, er dette en konstatering eller mangler der noget tekst
3.1;13	Webservicen definerer med andre ord sit eget datasæt (egen facade)	Dette siger blot at en facade kan udstilles med WS og er ikke relavant for R03
3.1;13	gennemstiller data direkte	Hvad vil det sige at gennemstille?

3.1;13	Såfremt data udstilles af webservicen som en facade, så vil ændringer til bagvedliggende webservices ikke påvirke serviceanvendere, medmindre facaden ændres.	Dette siger blot at en facade kan udstilles med WS og er ikke relavant for R03
3.2;14	Ved integrationer mellem forskellige myndigheders it-systemer er det centralt, at ansvaret for gennemførsel og fejlhåndtering ved en transaktion er tydeligt placeret.	Fyld – ikke specielt for myndigheder – fokuser på webservices som er emnet for nærværende dokument.
3.2;14	hvor funktionaliteten medfører overdragelse af ansvar mellem myndigheder.	Virker som en konstatering og er sat generelt op, hvilket kan få mislyde hvad angår persondataforordningen. Hvorfor tales der kun om funktionalitet og ikke om data?
3.2;14	En webservice skal entydigt kunne håndtere gentagne forsøg fra serviceanvenderen.	Retningslinien er korrekt , men praktisk vil det kræve at ws er i stand til at håndtere dubletter, hvorfor retningslinien anbefales at være Valfrit idet mange eksisterende implementationer ikke kan håndtere dubletter.
3.3;17	Opmærk	Konkretisering af begrebet "Opmærkning" ønskes Det skal allerede på nærværende niveau være klart hvad dette indebærer eller om der blot er tale om "at angive" Uden at begræbet er forblaret er det uklart om princippet efterleves korrekt Denne kommentar skal også ses i sammenhæng med forviringen mellem "retningslinier" og "skal" som angivet i tidligere kommentar til dokukmentet
3.5;23	Webservices skal logge et unikt requestID ved hvert kald, og ved gensendelse af et svar skal samme RequestID anvendes.	Retningslinien synes at håndtere 2 ting på samme tid: 1) Hvad der skal logges 2) Hvilke informationer webservicen skl indeholder , her requestID For at være i harmoni med R14 bør kun punkt 2) berøres medens 1) skal placeres i et andet princip
3.5;23	Entydighed	Som det implicit er angivet fødes requestID hos anvenderen og kan kun forlanges entydig i denne

		kontekst. entydighed kunne evt skabes ved en myID/youID tilgang Alternativt kan man tale om global entydighed, dvs. på tværs af systemer indenfor en arkitektur (f.eks. den fællesoffentlige)
3.6;24	kræver ingen sikkerhedsmæssige rettigheder hos serviceanvenderen.	Det skal i højere grad understreges at det selvfølgelig kun er anvenderen af kerne-servicen der har adgang til monitorerings servicesen, hvis ikke ville det jo være en indgang for en angriber at verificere succes eller ej af angrebet
3.6;25	Det er centralt, at monitoreringen ikke foretager opdateringer i data.	Ligeledes er det centralt at servicesens sikkerhed ikke forringes derved
3.9;33	af SAML 2.0	SAML-token skal vel være signerede?
3.9;33	og Transport layer security	Hvorfor kun sikkerhed på transportlaget, det kunne være rart med nogle retningslinier som også inddrager integritet: 1) for end-to-end eller peer-to-peer sikkerhed 2) for signering 3) for SAML2.0 profiler (OASIS)
4.1;34	Serviceanvendere har typisk behov for anvendelse af udstillede webservices i forbindelse med gennemførsel af en forretningsproces i organisationen.	En noget vovet generalisering Disse 6 linier virker som fyld og giver ikke megen værdi
4.1;34	REST webservices skal udstille data som ressourcer,	Hvorfor denne begrænsning? Wikipedia's bud: " "Web resources" were first defined on the World Wide Web as documents or files identified by their URLs, but today they have a much more generic and abstract definition encompassing every thing or entity that can be identified, named, addressed or handled, in any way

		whatsoever, on the Web"
4.1;34	. [REST].	Referencen findes ikke
4.1;35	REST webservices udstiller data som ressourcer,	Hvorfor denne begrænsning? Wikipedia's bud: " "Web resources" were first defined on the World Wide Web as documents or files identified by their URLs, but today they have a much more generic and abstract definition encompassing every thing or entity that can be identified, named, addressed or handled, in any way whatsoever, on the Web"
4.5;47	Sikkerhedskrav til REST webservices	Hvordan sikres complience til persondataforordningen? Det kunne være rart med nogle retningslinjer hvad angår integritet: 1) for end-to-end eller peer-to-peer sikkerhed 2) for signering