



Sammenhæng

Valg af webservice-standard i det offentlige - Implementeringsmodel for forretningservices



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling



Valg af webservice-standard i det offentlige
- Implementeringsmodel for
forretningsservices

Udgivet af:

IT- & Telestyrelsen
IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø
Telefon: 3545 0000
Fax: 3545 0010

Publikationen kan også hentes på IT- &
Telestyrelsens hjemmeside:

<http://www.itst.dk>

Tryk: Grefta Tryk

ISBN 978-87-92311-28-3

>

Valg af webservice-standard i det offentlige

Implementeringsmodel for
forretningservices

Indhold

>

Indledning	7
Forord	7
Formål med implementeringsmodellen	7
Mønstre for anvendelse af webservices	7
IT- og Telestyrelsens koordinerende rolle	8
Internationale WS standarder og OIO Webservice	
Profiler	8
Toolkits og referenceimplementeringer	8
Optagelse af standarder	8
Målgruppe	9
Mønstrenes status	9
Identificeret	9
Under udvikling	9
Etableret	9
Læsevejledning	9
Oversigt over implementeringsmodellens mønstre	10
Offentlige data	12
Mål	12
Motivation	12
Kontekst	12
Løsning	12
Struktur og deltagere	12
Konsekvenser	12
Vejledninger og profiler	12
Kendte anvendelser	13
Mine data	14
Mål	14
Motivation	14
Kontekst	14
Løsning	14
Struktur og deltagere	14
Konsekvenser	14
Vejledninger og profiler	14
Mine data via intermediær	15
Mål	15
Motivation	15
Kontekst	15
Løsning	15
Struktur	16
Eksempel	16
Deltagere	16
Konsekvenser	16
Vejledninger og profiler	17
Kendte anvendelser	17
Relaterede mønstre	17
Dokumentforsendelse	18
Mål	18
Motivation	18
Løsning	18

Modtager etablerer webservice – mønster	19
Struktur og deltagere	19
Løsning	19
Kontekst	19
Konsekvenser	19
Vejledninger og profiler	19
Kendte anvendelser	19
Afsender etablerer webservice – mønster	20
Struktur og deltagere	20
Løsning	20
Kontekst	20
Konsekvenser	20
Vejledninger og profiler	20
Kendte anvendelser	21
Hverken afsender eller modtager etablerer en webservice – mønster	22
Struktur og deltagere	22
Løsning	22
Kontekst	22
Konsekvenser	22
Vejledninger og profiler	22
Kendte anvendelser	23
Store datamængder	24
Mål	24
Motivation	24
Kontekst	24
Løsning	24
Struktur	25
Eksempler på anvendelser	25
Konsekvenser	25
Vejledninger og profiler	25
Abonnement på hændelser	26
Mål	26
Motivation	26
Kontekst	26
Løsning	26
Struktur	27
Eksempel	27
Deltagere	27
Konsekvenser	28
Vejledninger og profiler	28
Kendte kommende anvendelser	28
Sikker forbindelse fra punkt til punkt	29
Mål	29
Motivation	29
Kontekst	29
Løsning	29
Struktur	29
Eksempel	29
Deltagere	30
Konsekvenser	30
Vejledninger og profiler	30
Kendte anvendelser	31
Forbindelse med beskedbaseret sikkerhed	32
Mål	32
Motivation	32
Kontekst	32
Løsning	32
Struktur	33

Eksempel	33
Deltagere	33
Konsekvenser	33
Vejledninger og profiler	34
Kendte anvendelser	34
Appendiks A: Relevante fælleskomponenter	35
openUDDI	35
Anvendelse i e-handel	35
Detaljer om OpenUDDI	35
Appendix B: Referencer og links	36
Appendix C: Proces for udvikling af indhold til implementationsmodellen	37
Konstatering af behov	37
Vurdering af potentialet for fælles infrastruktur	38
Afholdelse af interessent-workshops	38
Beslutning om hvorledes behov adresseres	38
Udarbejdelse af implementerbar standard	38
Kvalitetssikring af udkast til profil	39
Offentlig høring	39
Udvikling og dokumentation af referenceimplementering	39
Kvalitetssikring af referenceimplementering	39
Inkludering i implementationsmodel	40
Opfølgende aktiviteter	40
Verifikation af overholdelse	40
Udvikling af vejledninger, fælleskomponenter og yderligere integrationsmønstre	41
Yderligere mønstre til implementationsmodellen	42
Vejledninger	43
Fælleskomponenter	43

Forord

Denne publikation er den første af 3 implementeringsmodeller, som udgives af Center for Serviceorienteret Infrastruktur (CSI) under IT- og Telestyrelsen:

- > Implementeringsmodel for forretningsservices (denne publikation)
- > Implementeringsmodel for brugerstyring (udkommer ultimo 2008)
- > Implementeringsmodel for forretningsprocesser (udkommer primo 2010)

Implementeringsmodellerne er væsentlige leverancer i forhold til etableringen af en sammenhængende IT-infrastruktur, som beskrevet i ”Visioner og milepæle for en National IT-infrastruktur”.

Implementeringsmodellen udbygges løbende. Den gældende version findes på www.itst.dk¹. Denne publikation indeholder et ”snapshot” af modellen i første kvartal 2008.

Formål med implementeringsmodellen

Målet med denne ”implementeringsmodel for forretningsservices” er at bistå offentlige myndigheder og private virksomheder med deres valg af *webservice-profil* i forbindelse med eksponering af services og registre samt udveksling af forretningsdokumenter. En webservice-profil er en specialisering af en webservice-standard i forhold til et givet formål. I vores tilfælde er formålet at fungere i en dansk serviceorienteret infrastruktur.

Behovet kan fx opstå i en situation, hvor en offentlig myndighed ønsker, at udveksle data med andre offentlige myndigheder og evt. private virksomheder eller f.eks. udstille et register. Her er det tanken, at implementeringsmodellen skal give svar på hvilken webservice-profil der bør anvendes.

Mønstre for anvendelse af webservices

Implementeringsmodellen beskriver en række mønstre for anvendelse af webservices. Det er ambitionen at mønstrene skal dække de mest almindelige anvendelsesscenarier for webservices, men det vil ikke være alle mønstre, hvor implementeringsmodellen kan pege på en konkret webservice-profil.

Mønstrene i implementeringsmodellen skal opfattes som et forsøg på kortlægning, hvor visse områder i en periode fremover vil være ”uudforskede”. Hvis en offentlig myndighed eller en privat virksomhed står med et konkret behov for at få udviklet en webservice profil for et af de områder, hvor der endnu ikke findes en standardiseret profil, bør anvendelse af webservices efter det valgte mønster ske efter koordination med Center for Serviceorienteret Infrastruktur hos IT og Telestyrelsen.

¹ <http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/implementeringsmodeller/implementeringsmodel-for-forretningsservices>

IT- og Telestyrelsens koordinerende rolle

Med udgivelse og vedligeholdelse af implementeringsmodellen ønsker IT- og Telestyrelsen at koordinere udviklingen af webservice profiler i Danmark. Koordinationen varetages i Center for Serviceorienteret Infrastruktur (CSI), som løbende vil vedligeholde implementeringsmodellen i takt med at der kommer nye standarder til, standardiseringsarbejdet er åbent for alle for information om deltagelse se www.itst.dk.

Internationale WS standarder og OIO Webservice Profiler

Implementeringsmodellen kan pege på profiler af webservice-standarder, som er blevet udviklet og vedligeholdes af forskellige organisationer. Ideelt set peger modellen kun på profiler af anerkendte internationale standarder med bred leverandørunderstøttelse. Desværre er det langt fra alle mønstre, hvor der findes internationale standarder, og i de fleste tilfælde er der behov for en dansk ”profilering”. Webservice-standarder, som er blevet ”profileret” og vedligeholdes af IT- og Telestyrelsen, er kendt som OIO Webservice Profiler.

Toolkits og referenceimplementeringer

IT- og Telestyrelsen har afsat ressourcer til at sikre de udpegede webservice-profiler i implementeringsmodellen også lever op til kravet om platformneutralitet. Med andre ord vil en profil ikke blive optaget i implementeringsmodellen med mindre, at det har været demonstreret, at der kan skabes løsninger, som er interoperable på tværs af relevante platforme, som fx Java- og .Net-platformen.

Udover at referere til profiler af standarder, dokumentation, vejledninger og best practices, så refererer implementeringsmodellen ligeledes til toolkits og referenceimplementeringer. Samlet set er målet at hjælpe udviklere hurtigere i gang med anvendelsen af standard-profilerne, og samtidig stille kode til rådighed, som gør det muligt, at teste egne løsningers interoperabilitet.

Optagelse af standarder

En webservice-profil kan optages i implementeringsmodellen efter vurdering af en række forhold.

- > Profilen skal være veldokumenteret og entydig.
- > Profilen skal være udviklet gennem en åben proces med inddragelse af toneangivende leverandører og offentlige myndigheder.
- > En eller flere offentlige myndigheder skal have konkrete forretningskrav, som profilen hjælper med at opfylde.

En profil som optages i implementeringsmodellen vil typisk også findes i OIO kataloget, som er kataloget over standarder for digital forvaltning.

Læs mere om optagelsesprocessen senere i dette dokument i ”Appendix C: Proces for udvikling af indhold til implementationsmodellen”.

Målgruppe

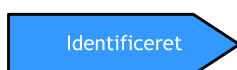
Implementeringsmodellen henvender sig til it-arkitekter, udviklere og tekniske projektledere. Det forudsættes at læseren har en almen viden om webservice teknologier og forstår de parametre, der er udslagsgivende for valg af den ene standard frem for en anden.

Mønstrenes status

Implementeringsmodellens mønstre er ikke alle lige veletablerede. For nogle af mønstrene er behovet for dem blot identificeret, andre af mønstrene er under udvikling hos CSI og endelig der de mere veletablerede mønstre, som er anvendt i konkrete implementeringer. For at kunne afgøre hvor i forløbet et givet mønster er - hvilken status det har - anvendes en følgende klassifikation. Mønsterets status kan antage 3 forskellige tilstande: *Identificeret*, *Under udvikling* og *Etableret*.

Identificeret

For at et mønster kan komme på tale som et mønster i implementeringsmodellen, skal det løse en central problemstilling indenfor integration i Det Digitale Danmark. At et mønster er identificeret betyder, at behovet for løsning af den problemstilling, der afspejles i mønsteret, er erkendt. At et mønster er identificeret udtrykkes grafisk med følgende figur:



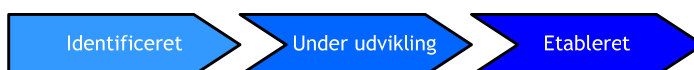
Under udvikling

At et mønster har status *Under udvikling* betyder, at behovet for mønsteret er identificeret, samt at der i CSI arbejdes på at færdiggøre mønsteret i en sådan grad at det kan anvendes i konkrete implementeringer. At et mønster er under udvikling udtrykkes grafisk på følgende måde:



Etableret

At et mønster har status *Etableret* betyder, at mønsteret er beskrevet samt, at det er anvendt i en eller flere implementeringer. At et mønster er etableret udtrykkes grafisk på følgende måde:










Læsevejledning

Næste afsnit indeholder en tabel med en oversigt over de mønstre som indgår i implementeringsmodellen. Det er ambitionen, at oversigten skal give et overskueligt overblik, således at læseren kan springe direkte ned til det mønster som bedst matcher en problemstilling.



De følgende afsnit beskriver de forskellige mønstre og evt. relevante webservice-standarder og -profiler mere detaljeret. Implementeringsmodellen afsluttes med en beskrivelse af fælleskomponenter, vejledninger og mønsterudviklingsprocessen,

Oversigt over implementeringsmodellens mønstre

>

Mønster	Mål	Variant	WS Profil	Status
Offentlige data	Udstilling af ikke personfølsomme data for alle.		OIOREST	Under udvikling 
Mine data	At give adgang til egne data for borgere og virksomheder.		OIOREST	Identificeret 
Mine data via intermediær	At understøtte selvbetjeningsløsninger, hvor data hentes fra 3. part med brugerens identitet.		OIOIDWS	Under udvikling 
Dokumentforsendelse	Sikker og pålidelig udveksling af potentielt personfølsomme dokumenter.	Service hos modtager	OIORASP	Etableret 
		Service hos afsender	OIOREST OWSA T	Under udvikling 
		Neutral kømekanisme		Identificeret 
Store datamængder	Sikker udveksling af store potentielt personfølsomme datamængder.		OIOXLWS	Under udvikling 
Abonnering på hændelser	At give systemer mulighed for at abonnere på hændelser som indtræffer i eksterne systemer.			Identificeret 

>

Sikker forbindelse fra punkt til punkt	At etablere en sikker punkt-til-punkt forbindelse mellem to sikkerhedsdomæner.		OWSA Model T	Etableret 
Forbindelse med beskedbaseret sikkerhed	At etablere en forbindelse, hvor sikkerheden etableres på beskedniveau.		OIOBSP	Under udvikling 

Offentlige data



>

Mål

At gøre offentlige data let tilgængelig uanset hvilken platform eller enhed (device), der skal anvende de offentlige data. Med offentlige data menes data, som kan stilles til rådighed for alle, uden at overtræde nogen sikkerhedsmæssige forskrifter.

Motivation

Myndighederne ligger inde med mange forskellige offentlige data, der kan anvendes i mange sammenhænge, hvis de blev gjort tilgængelige. Mangfoldigheden af enheder, der har behov for at anvende de offentlige data, er stor: PC'er, servere, mobiltelefoner, PDA'er osv. For at undgå at myndighederne skal etablere løsninger for hver enkelt platform ønskes en løsning, som kan anvendes af et så stort udsnit af enheder som muligt.

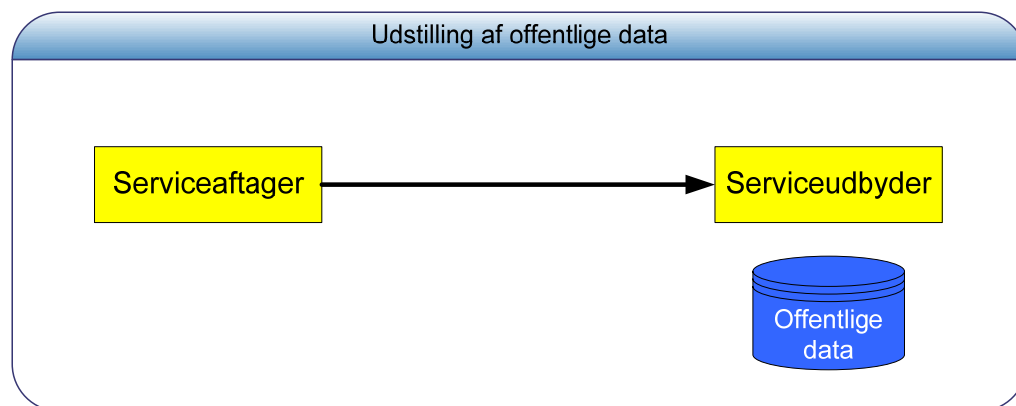
Kontekst

Mønsteret kan anvendes i forbindelse med at offentlige data ønskes gjort bredt tilgængelig.

Løsning

De offentlige data udstilles vha. af en REST² baseret webservice.

Struktur og deltagere



Konsekvenser

De offentlige data gøres tilgængelige for enhver applikation, platform og enhed (device) som kan håndtere HTTP og XML.

Vejledninger og profiler

OIOREST Basis (Udgives første halvår af 2008)

CSI er i øjeblikket i færd med at eksperimentere med at udstille offentlige data vha. REST baserede webservices. Der udvikles en REST baseret webservice, [Danmark webservicen](http://oiorest.dk/danmark/) (<http://oiorest.dk/danmark/>), som udstiller information om forskellige

² REST er en arkitektonisk stil, hvor forkortelsen står for Representational State Transfer.

>

dele af Danmark: regioner, kommuner, sogne, postdistrikter, valgdistrikter, skoledistrikter, grundskoler, veje og adresser (over 2,2 millioner).

Kendte anvendelser

Google stiller deres kort til rådighed via en REST baseret webservice: [Google Static Maps](http://code.google.com/apis/maps/documentation/staticmaps/index.html) (<http://code.google.com/apis/maps/documentation/staticmaps/index.html>)

Mål

At gøre myndigheders og andres organisationers data vedrørende borgere / virksomheder tilgængelig for borgeren / virksomheden selv. Data gøres tilgængelig på en standardiseret måde, med henblik på at de kan tilgås fra et bredt udsnit af applikationer, enheder og platforme. Med mine data menes data vedrørende en borger/virksomhed, som er belagt med sikkerhedsforskrifter, men kan stilles til rådighed for borgeren/virksomheden selv.

Motivation

Borgere og virksomheder har data vedrørende dem selv liggende i myndigheders og andre organisationers registre. Disse data kan med fordel anvendes af borgeren/virksomheden selv i andre sammenhænge. Borgeren kan f.eks. ønske at sammenstille sine økonomiske data fra forskellige steder Skat, kommunen, banken, el-selskab osv. i sit privatøkonomiprogram.

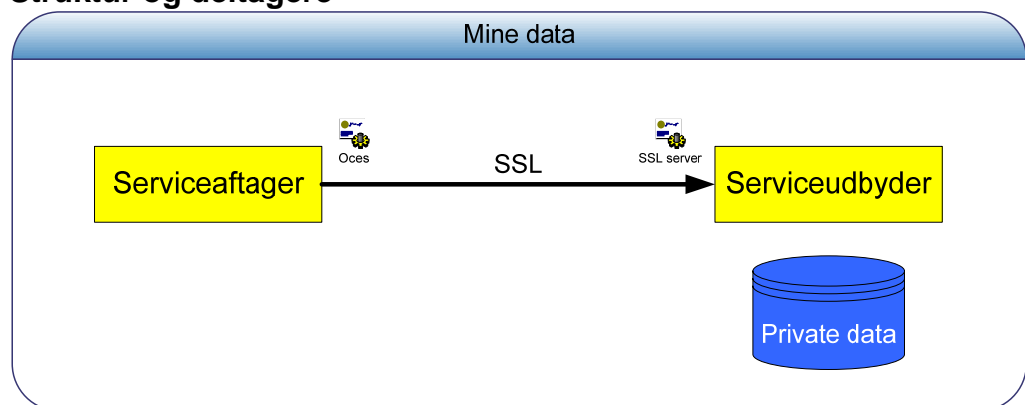
Kontekst

Mønsteret anvendes i forbindelse med at give borgere og virksomheder adgang til data om dem selv.

Løsning

En mulig løsning vil være at de private data udstilles vha. af en REST baseret webservice, hvor autenticiteten etableres vha. OCES certifikater/SAML og fortrolighed etableres med en SSL forbindelse mellem borgeren/virksomheden og organisationen med de ønskede data. Det skal afklares hvorvidt mønsteret kan anvendes i portalsammenhænge.

Struktur og deltagere



Konsekvenser

Private data om borgere/virksomheder gøres tilgængelig for borgeren/virksomheden selv på en sikker og fortrolig måde.

Vejledninger og profiler

OIOREST Basis (Udgives første halvår af 2008)

OIOREST med sikkerhed (Udgives andet halvår af 2008)

Få mere information under OIOREST på <http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices>

Mål

At gøre myndigheders og andres organisationers data vedrørende borgere/virksomheder tilgængelig for serviceaftagere, som handler på borgerens/virksomhedens vegne. Data gøres tilgængelig på en standardiseret måde, med henblik på at de kan tilgås fra et bredt udsnit af applikationer, devices og platforme. Med mine data menes data vedrørende en borger/virksomhed, som er fortrolige og eventuelt også følsomme i persondatalovens betydning, men som kan stilles til rådighed for, og videreanvendes i en serviceaftager-løsning som agerer på borgerens/virksomhedens vegne.

Motivation

Såvel indenfor det offentlige som i den private sektor er der stort potentiale i form af effektiviseringer og kvalitetsforbedringer ved at støtte ansøgnings- og anskaffelsesprocesser med digitale selvbetjeningsløsninger. En væsentlig gevinst ligger i at en stor del af nødvendige data allerede findes i andre it-løsninger. Ved at hente disse data direkte fra kilden spares der umiddelbart tid og det er ikke nødvendigt efterfølgende via manuelle processer at validere at data er korrekte. De data, der er tale om er oftest data, som ansøgeren betragter som private, og der kan også være tale om data, der er følsomme ifølge persondataloven, eksempelvis ved ansøgninger, hvor ansøgerens straffeattest skal vedlægges, adgang til egen sag hos kommunen, etc. Ligeledes er en række processer, hvor andre end dataejer (fx en sagsbehandler) tilgår private/følsomme data i eksterne systemer/registre, hvor det er vigtigt at kunne logge præcis hvilken bruger det er, der har tilgået data.

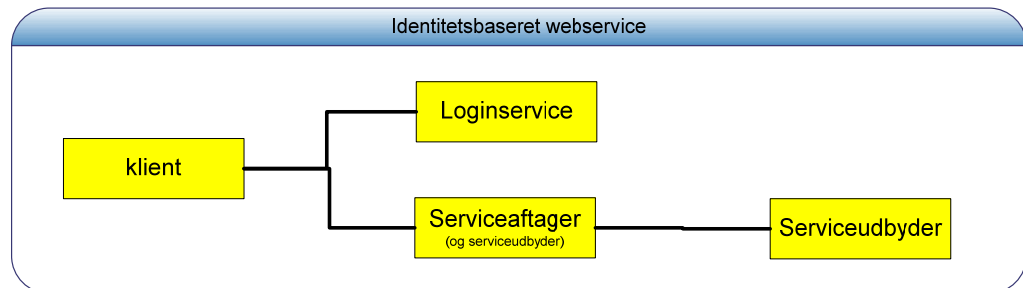
Kontekst

Mønsteret anvendes hvor brugeren tilgår en løsning, som anvender eksterne data, som den data-afgivende service kun vil give adgang til under følgende betingelser: Der skal leveres bevis for at den bruger forespørgsel foretages på vegne af rent faktisk er logget ind ved afsendelse af forespørgslen, og der skal evt. være mulighed for at bede brugeren bekræfte at data må afgives.

Løsning

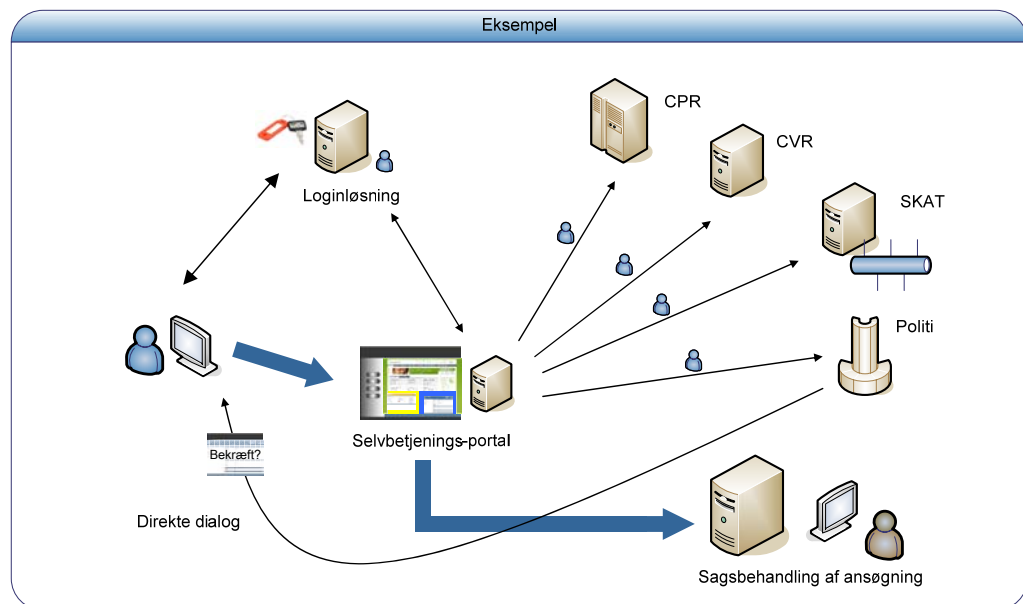
Det muliggøres at den oprindelige brugers identitet bibeholdes i et webservicekald, som udføres på vegne af brugeren. Den løsning, hvor brugeren logger ind (kaldet Identity Provider) opretter og signerer et security token med brugerens identitet, som en serviceaftager kan anvende til at udstede et webservice-kald med, som er sikret med WS-Security standarden. Serviceudbyderen modtager således en anmodning på vegne af en bruger, som Identity Provideren står inde for rent faktisk er logget ind. Hvis der er behov for at validere at brugeren er indforstået med den konkrete data-anmodning/transaktion er det muligt for serviceudbyderen (den data-afgivende service) at bede om direkte interaktion med brugeren, som så kan bekræfte at data-anmodning/transaktion skal gennemføres.

Struktur



Eksempel

Figuren herunder illustrer et eksempel på en selvbetjeningsløsning, hvor ansøgeren med sin egen identitet henter nødvendig dokumentation fra en række myndigheder, hvorefter ansøgningen når den er komplet og valideret kan sendes til sagsbehandling hos relevante myndighed/virksomhed.



Deltagere

Deltagerne er

- Loginløsning (Identity Provider), som kontrollerer brugerens akkreditiver
- Serviceudbyder, som stiller data og/eller services til rådighed
- Serviceaftager, som kalder serviceudbyder på vegne af bruger, der er logget ind hos login-løsningen

Konsekvenser

Det er muligt at lave it-løsninger, som kun kan sammenstille personlige data fra flere kilder når dataejer er involveret.

Løsningen forudsætter at der via aftaler og fælles politikker er tillid mellem den "Identity Provider", der logger brugeren ind, og dataafgivende løsning. Løsningen sikrer på det tekniske niveau basalt at en webservice-aftager ikke kan foretage et

>

webservicekald på vegne af en bruger uden at denne bruger er logget ind og har en aktiv session.

Vejledninger og profiler

- > OIOWS - Kommende OIO profil for identitetsbaserede webservices
- > Teknisk vejledning om sikring af digitale signaturers bevisværdi (<http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-loesninger/signatur-og-systembeviser>)
- > Vejledning for udvikling og anvendelse af OIOWSDL (<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oiowSDL-kontrakt-forst-udvikling-med-oioxml>)
- > OIO Standardkontrakt for webservices. Skabeloner til SLA-aftaler findes i kontraktens bilag (<http://www.itst.dk/arkitektur-og-standarder/arkitektur/serviceorienteret-arkitektur/webservices/standardkontrakt-for-webservices/>)

Kendte anvendelser

Ingen i produktion. Færdselsstyrelsen har foretaget *proof of concept* på en løsning til ansøgning om transporttilladelse.

Relaterede mønstre

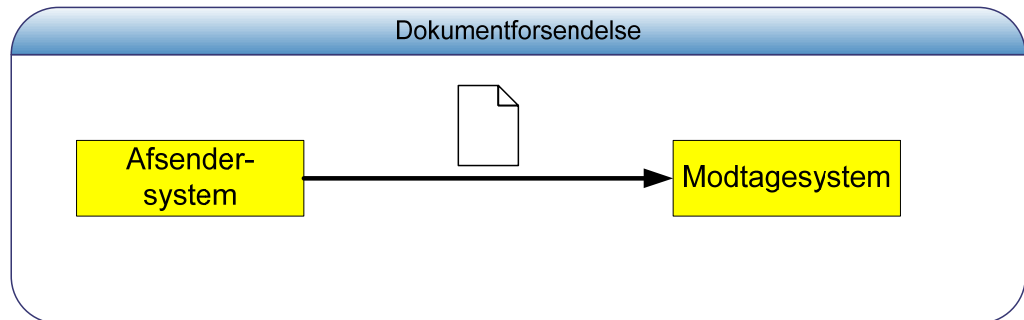
OIOBSP (OIO Basic Security Profile) udgør også en del af dette mønster.

Dokumentforsendelse

>

Mål

At kunne sende et dokument sikkert og pålideligt fra en afsender til en modtager. Med sikkert menes at både afsender og modtager af dokumentet autentificeres samt at kommunikationen er fortrolig. Med pålideligt menes at der i løsningen kan etableres en mekanisme til at sikre at dokumentet er leveret til modtager.



Motivation

Der er i mange forbindelser behov for digitalt at kunne sende et dokument mellem to parter. Som eksempler kan nævnes tinglysningsdokumenter, fakturaer, ordrer, forskellige former for opgørelser. Behovet er også kommet til udtryk i flere offentlige digitaliseringsprojekter, som f.eks. Dokumentboks, NemSMS og NemHandel.

Løsning

Løsningen afhænger af de deltagende parter digitale muligheder samt rationale i at etablere en webservice. Der kan være forskellige grunde til at en eller begge af de kommunikerende parter ikke ønsker at etablere en webservice, som f.eks.:

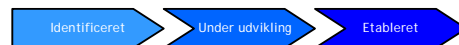
- > Ingen økonomisk fordel
- > Manglende teknologisk erfaring/viden

Af denne grund er løsningen opdelt i tre undermønstre:

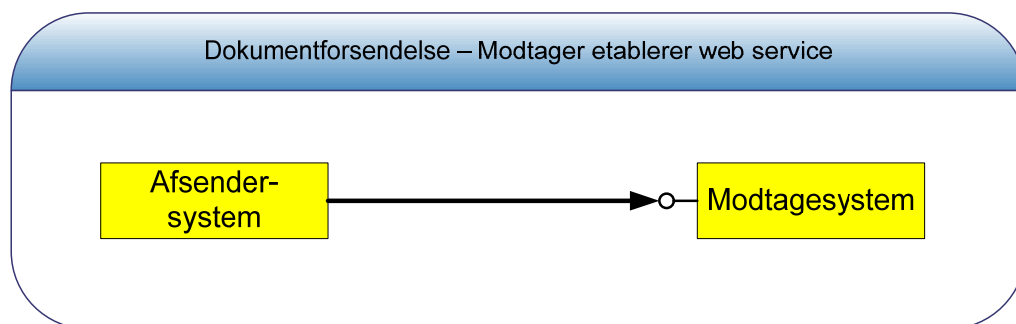
- > Modtager har mulighed for at etablere en webservice
- > Afsender har mulighed for at etablere en webservice
- > Hverken afsender eller modtager har mulighed for at etablere en webservice.

>

Modtager etablerer webservice – mønster



Struktur og deltagere



Løsning

Modtager etablerer en webservice, som afsender anvender til at sende dokumenter. Kommunikationsformen følger OIORASP profilen.

Kontekst

Mønstret anvendes i forbindelse med udveksling af forretningsdokumenter i NemHandel, men kan anvendes generelt i forbindelse med at dokumentmodtager har rationale/fordel i at etablere en webservice.

Konsekvenser

Dokumenter kan udveksles sikkert og pålideligt mellem partnere over internettet.

Vejledninger og profiler

- > OIORASP (<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oio-rasp-sikker-og-palidelig-datatransport>)
- > Vejledning for udvikling og anvendelse af OIOWSDL (<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oiowSDL-kontrakt-forst-udvikling-med-oioxml>)
- > OIO Standardkontrakt for webservices. Skabeloner til SLA-aftaler findes i kontraktens bilag (<http://www.itst.dk/arkitektur-og-standarder/arkitektur/serviceorienteret-arkitektur/webservices/standardkontrakt-for-webservices/>)

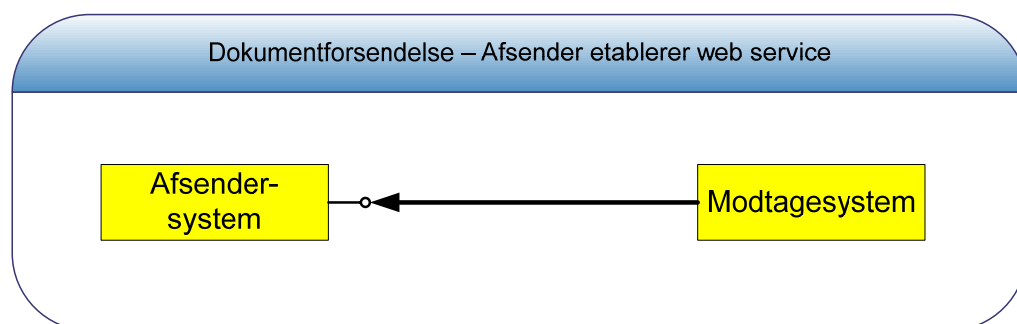
Kendte anvendelser

NemHandel er et oplagt eksempel på både anvendelsen af mønstret samt anvendelse af OIORASP (<http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/nemhandel>).

Afsender etablerer webservice – mønster



Struktur og deltagere



Løsning

Afsender etablerer en webservice, som modtager med mellemrum anvender til for at undersøge om afsender ønsker at sende dokumenter. Hvis afsender har dokumenter til modtager returneres disse af webservices. OWSA model T eller OIOREST kan anvendes som kommunikationsform. Som overordnet regel anvendes OIOREST, når løsningen skal kunne anvendes af flest mulige typer klientapplikationer/platforme. OWSA model T når omgivelserne (platform, applikationer, værktøjer og andre faktorer) peger på en SOAP baseret kommunikation. Dette skal dog kun opfattes som en grov tommelfingerregel. Det faktiske valg kræver en større indsigt i den konkrete kontekst, som løsningen skal fungere i.

Kontekst

Mønsteret kan anvendes hvis afsender ser et rationale i at tilbyde denne form for kommunikation til modtagere, som ikke har mulighed for at etablere en webservice til modtagelse af dokumenter.

Konsekvenser

Modtager skal med passende mellemrum kalde afsenders webservice for at afgøre om der er dokumenter til vedkommende. Modtager får ingen direkte information om dokumentet er modtaget hos modtageren. Hvis afsenderen har dette behov skal der etableres en mekanisme (webservice), således at modtageren kan sende kvitteringer til afsenderen.

Vejledninger og profiler

- > OWSA model T
(<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oio-web-service-arkitekturen>)
- > Vejledning for udvikling og anvendelse af OIOWSDL
(<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oiodsdl-kontrakt-forst-udvikling-med-oioxml/?searchterm=oiowsdl>)

>

- > OIO Standardkontrakt for webservices. Skabeloner til SLA-aftaler findes i kontraktens bilag (<http://www.itst.dk/arkitektur-og-standarde/arkitektur/serviceorienteret-arkitektur/webservices/standardkontrakt-for-webservices/>)
- > OIOREST Basis (Udgives første halvår af 2008)
- > OIOREST med sikkerhed (Udgives andet halvår af 2008)
- > Få mere information under OIOREST på <http://www.itst.dk/arkitektur-og-standarde/Standardisering/standarde-for-serviceorienteret-infrastruktur/standarde-for-webservices>

Kendte anvendelser

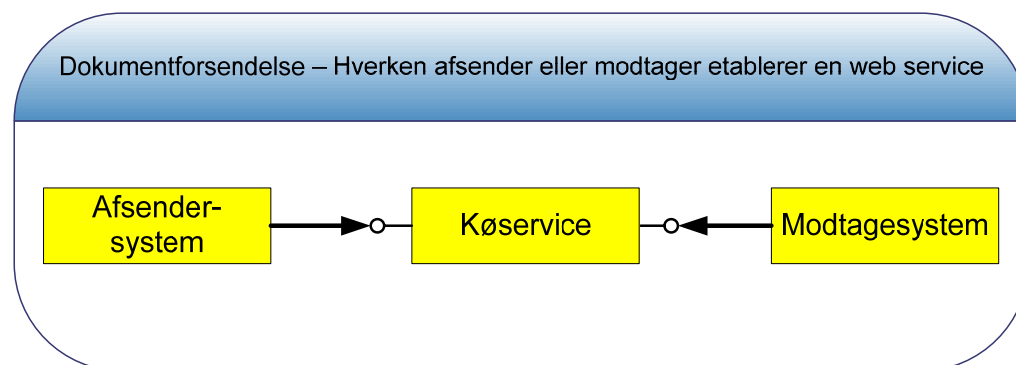
Web feed³ er et kendt eksempel på at dokumenter hentes hos afsender.

³ En beskrivelse af web feed kan ses på http://en.wikipedia.org/wiki/Web_feed

Hverken afsender eller modtager etablerer en webservice – mønster

Identificeret

Struktur og deltagere



Løsning

Der etableres en offentlig central køservice, som kan mellemlagre dokumenter. Der skal gøres opmærksomhed på at en sådan service ikke eksisterer. Hvis en køservice etableres er der hverken behov for at afsender eller modtager etablerer en webservice. Afsender sender dokumentet til modtagerens kø i køservicen. Herefter kan modtageren undersøge hvorvidt der ligger dokumenter i sin kø i køservicen, og hvis det er tilfældet hente det.

Kontekst

Mønsteret kan anvendes hvor hverken afsender eller modtager har et rationale i etablere en webservice til kommunikation af dokumenter. Mønsteret har den fordel, at når køservicen er etableret kan digitalisering af dokumentforsendelse billiggøres for tjenester med lille transaktionsvolumen. Ligeledes kan køen anvendes til kapacitet udjævning i modtagersystemet.

Konsekvenser

Hverken afsender eller modtager skal etablere en webservice for at kunne sende dokumenter til hinanden..

Vejledninger og profiler

- > OIOREST Basis (Udgives første halvår af 2008)
- > OIOREST med sikkerhed (Udgives andet halvår af 2008)
- > CSI er i øjeblikket i færd med at eksperimentere med en REST baseret køservice (<http://oiorest.dk/queueservice>)
- > Få mere information på itst.dk om OIOREST (<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices>)

>

Kendte anvendelser

Reach – The Irish Government’s SOA Initiative (<http://www.reach.ie/>) samt Amazon Simple Queue Service (<http://www.amazon.com/Simple-Queue-Service-home-page/b?ie=UTF8&node=13584001>)

Mål

At gøre det muligt at udveksle store datamængder sikkert, robust og uafhængigt af platform eller enhed (device). Da der ofte er tale om personfølsomme oplysninger skal afsenderen kunne autentificeres og data skal kunne udveksles konfidentielt og med verificerbar integritet. Dertil kommer, at afsenderen i mange tilfælde ønsker en teknisk kvittering for at data er blevet udvekslet.

Motivation

Offentlige myndigheder udveksler i visse situationer store mængder data med andre offentlige myndigheder og private virksomheder. Tendensen har været, at store datamængder udveksles på fysiske medier eller via bilateralt aftalte protokoller, hvoraf flere har sikkerhedsmæssige svagheder. Tab af offentlige data i andre lande har været med til at synliggøre svagheden ved de eksisterende metoder. For at undgå, at myndighederne etablerer udvekslinger på ad hoc basis, hvor der kan være usikkerhed om hvorvidt de forretningsmæssige krav er opfyldt, ønskes en standardiseret og tilgængelig løsning som kan anvendes så bredt som muligt.

Kontekst

Mønsteret kan anvendes i forbindelse med udveksling af alle typer data herunder personfølsomme, hvor en kombination af båndbredde, mængden af data, og den tid det tager for udvekslingen, fordrer et asynkront udvekslingsmønster. Behov for synkron udveksling af store datamængder er ikke dækket af dette mønster.

Løsning

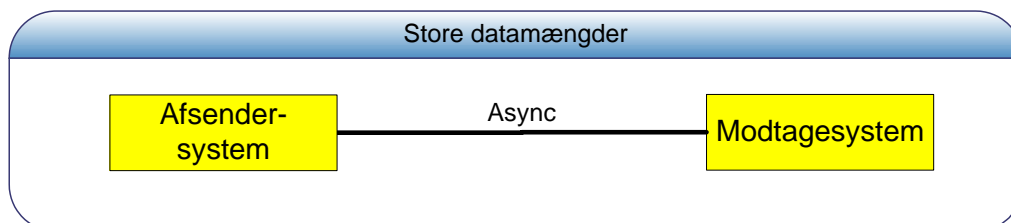
Asynkron udveksling af store mængder data baseret på åbne standarder sker i dag primært vha. FTP over SSL eller SSH FTP (S-FTP). MTOM⁴ betragtes af flere som et interessant alternativ i forhold til en anvendelse i webservice-scenarier. Danske erfaringer er dog begrænsede i forhold til MTOM.

Ved afleveringer / indberetninger fra et afsendersystem til et modtagesystem (push), er det modtagesystemet, der skal udbyde en service, som afsendersystemet kan aflevere data til. I andre scenarier er det afsendersystemet, som skal udbyde en service således, at modtagesystemet kan hente data (pull).

IT- og Telestyrelsen har i marts 2008 afholdt en indledende workshop om udveksling af store datamængder. Det er forventningen at dette arbejde skal lede til en egentlig profil for udveksling af store datamængder med arbejdstitlen, OIOXLWS.

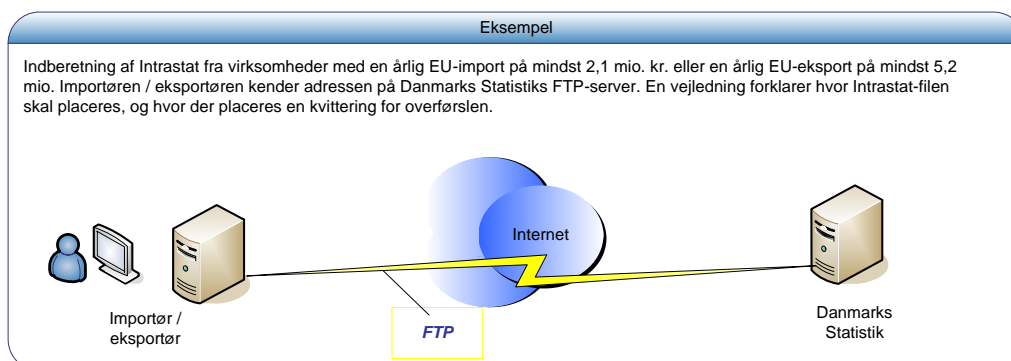
⁴ MTOM er forkortelsen for *Message Transmission Optimization Mechanism*

Struktur



Eksempler på anvendelser

- > Indberetning af intrastat til Danmarks Statistik⁵ via FTP.
- > Hentning af data fra det Centrale Virksomhedsregister via S-FTP.
- > Indberetning til LetLøn via FTP eller web upload



Konsekvenser

Ved anvendelse af FTP og S-FTP får afsenderen ikke formel kvittering på at data er blevet afleveret til modtagesystemet. Ønskes en sådan kvittering, skal der udarbejdes en kvitteringssemantik, som ligger ud over den basale protokol.

Vejledninger og profiler

Der er pt. ikke udarbejdet vejledninger eller profiler for udveksling af store datamængder. Center for Serviceorienteret Infrastruktur er i færd med at afdække de forretningsmæssige og ikke-funktionelle krav til en evt. profil på området.

⁵ Intrastat er statistikken, der beskriver Danmarks varehandel med EU. Virksomheder med en årlig EU-import er på mindst 2,1 mio. kr. eller en årlige EU-eksport er på mindst 5,2 mio. skal indberette til Intrastat. <http://www.dst.dk/Intrastat.aspx>

Abonnering på hændelser



Mål

At det er muligt på en standardiseret og enkel måde, at abonnere på hændelser som indtræffer i eksterne fagsystemer. Tilsvarende - at fagsystemer på en standardiseret måde kan notificere abonnenterne omkring de hændelser som der abonneres på.

Motivation

På tværs af den offentlige og private sektor har en række fagsystemer behov for information omkring hændelser, som indtræffer i andre fagsystemer. Fødsel eller dødsfald er eksempler på hændelser, hvor en række fagsystemer hos forskellige myndigheder skal have en notifikation. Ved fødsels skal det sikres, at det nyfødte barn får et navn og at familien får besøg af den kommunale sundhedsplejerske. Omvendt skal man ved dødsfald sikre, at der ikke længere sendes post til den afdøde. Andre eksempler er hændelser som optræder i forskellige fagsystemer, som skal registreres i et ESDH-system eller andre fagsystemer. Bevægelsen hen mod IT-systemer der er udviklet efter designprincipperne kendt fra Serviceorienteret Arkitektur, hvor funktionaliteten i en løsning udvikles som services og stilles til rådighed som elementer i en overordnet proces, hvor forretningsmoduler er afgrænsede og uafhængige, øger behovet for en standardiseret udveksling af hændelser. Uden en fælles standard på området, kan man stå i en situation, hvor et og samme fagsystem skal understøtte forskellige specifikationer for notifikation og abonnering med forøgede omkostninger til følge.

Kontekst

Mønstret anvendes i situationer, hvor man mellem fagsystemer ønsker at dele information om hændelser (begivenheder af forretningsmæssig karakter – også kaldet tilstandsskift), og hvor det er nyttigt, at der sker en asynkron afkobling i forhold til hændelseskilden.

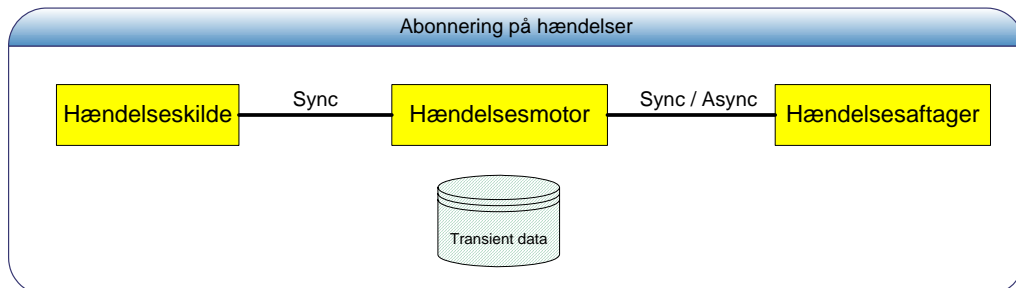
Løsning

Der er pt. ikke udarbejdet en standardiseret profil for hændelser. WS-Eventing fra OASIS synes at være den standard, der har mest momentum pt. Der er pt. ingen drifts-erfaringer med WS-Eventing i den offentlige sektor i Danmark, men fra den 1. juli 2007 idriftsættes en et pilotforsøg i Ringsted Kommune mellem IT- og Telestyrelsen, KMD og Traen, hvor de første erfaringer høstes.

En WS-Eventing baseret løsning fordrer etablering af en fælleskomponent kaldet en hændelsesmotor. Hændelsesmotoren fungerer som en neutral part mellem en hændelseskilde, som skaber en hændelse baseret på proces- eller tilstandsskift, og en hændelsesaftager, som udfører den opgave den varetager i forhold til de hændelser den abonnerer på.⁶ Hændelsesaftageren skal for sin part etablere en webservice, som kan kaldes af hændelsesmotoren når en hændelse som opfylder abonnementet indtræffer.

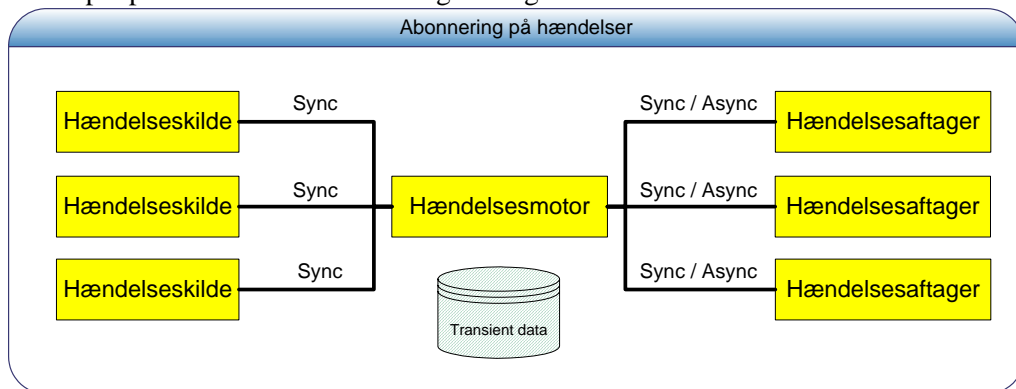
⁶ Kilde: <http://www.domstol.dk/e-TI/nyheder/ovrigenyheder/Pages/Haendelsesstyring.aspx>

Struktur

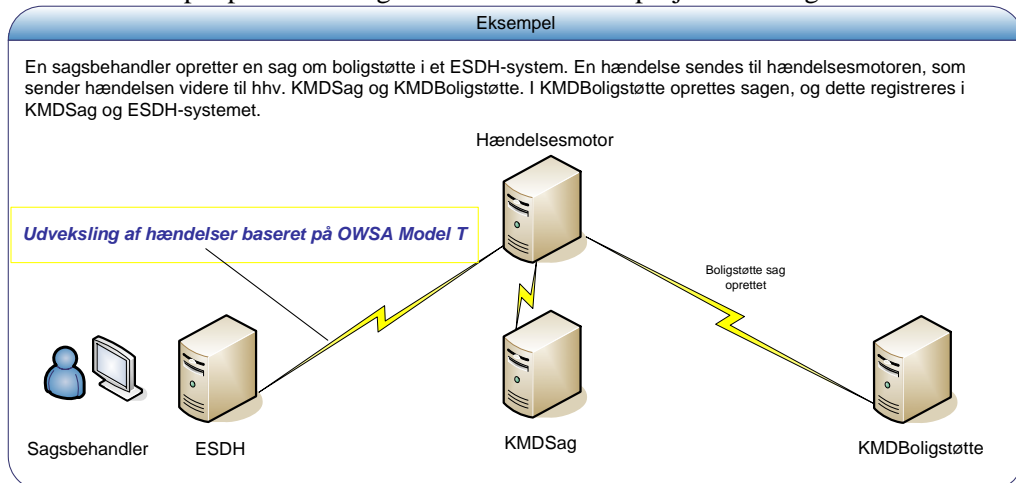


Eksempel

Eksempel på flere hændelseskilder og – aftagere:



Konkret eksempel på udveksling af hændelser i I-SD projektet i Ringsted kommune:



Deltagere

Deltagerne er

- > Hændelseskilde, hvor der indtræffer eller registreres et tilstandsskift.
- > Hændelsesmotor, som registrerer hændelser og sætter dem i kø for efterfølgende distribution til en eller flere hændelsesaftagere.

>

- > Hændelsesaftager, har ”tegnet abonnement” hos hændelsesmotoren på bestemte hændelser fra en eller flere hændelseskilder.

Konsekvenser

Det er muligt, at lave it-løsninger som i højere grad efterlever design-principperne omkring Serviceorienteret Arkitektur, hvor det tilstræbes, at forretningsmoduler er uafhængige og afgrænsede. Ved at indskyde en ”neutral” hændelsesmotor mellem uafhængige fagsystemer sikres det, at de enkelte systemer kan udskiftes, fjernes eller at nye systemer kan tilføjes efter behov.

Vejledninger og profiler

En dansk profilering af WS-Eventing forventes udviklet i første halvår af 2009.

Kendte kommende anvendelser

I Domstolsstyrelsens elektroniske Tinglysningssystem er det planlagt, at WS-Eventing skal anvendes til at styre udvekslingen af hændelser mellem den centrale tinglysningsmotor på den ene side, og banker, realkreditinstitutioner, ejendomsmæglere og advokater på den anden side. (<http://www.domstol.dk/e-Tl/nyheder/ovrigenyheder/Pages/Haendelsesstyring.aspx>)

I forhold til integrationen mellem ESDH-systemer og andre fagsystemer er der tilsvarende ved at ske en afprøvning af en hændelsesmotor. Dette sker i regi af I-SD pilotprojektet mellem ITST, KMD, KL, Ringsted Kommune og Traen. Her er man i færd med at implementere en hændelsesmotor som i første omgang sender hændelser til hændelsesaftagere baseret på OWSA Model T. For at begrænse projektets omfang er der valgt boligstøtte som praksisområde og at projektet realiserer et begrænset antal kørende integrationer mellem Traen ESDH Acadre og KMD-sag-basis plus KMD-boligstøtte. (<http://www.itst.dk/arkitektur-og-standarder/Standardisering/datastandardisering/fesd/integration-mellem-esdh-og-fagsystemer>)

Sikker forbindelse fra punkt til punkt



>

Mål

At etablere en sikker punkt-til-punkt forbindelse mellem to sikkerhedsdomæner, hvor der er én serviceaftager og én serviceudbyder.

Med sikker forbindelse menes her at serviceudbyder og -aftager kan autenticitetssikres og beskeder kan kommunikeres med integritet og fortrolighed.

Motivation

En række eksisterende og nye it-løsninger har behov for – via åbne net - at kunne lave opslag i, eller overføre data til andre systemer uden brud på fortrolighed og integritet. Der er behov for en ensartet måde at implementere sikre forbindelser mellem serviceaftager og serviceudbyder på. Dette skal kunne realiseres med eksisterende etablerede teknologier og standarder.

Kontekst

Mønsteret anvendes i forbindelse med integration mellem bestående løsninger hos myndigheder og leverandører, hvor det er tilstrækkeligt at webservice-kaldene udføres med systemernes identitet.

Løsning

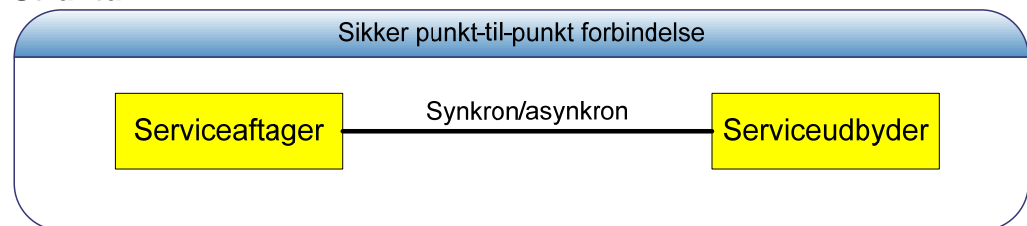
Sikker punkt-til-punkt forbindelse etableres i overensstemmelse med OWSA Model T profilen.

HTTPS benyttes til transport og sikkerhed. Transportlaget krypterer data og overfører certifikat mellem Serviceudbyder og Serviceaftager til autentifikation.

OCES certifikater benyttes som identifikation af Serviceaftager.

En Serviceudbyder identificeres med et Servercertifikat.

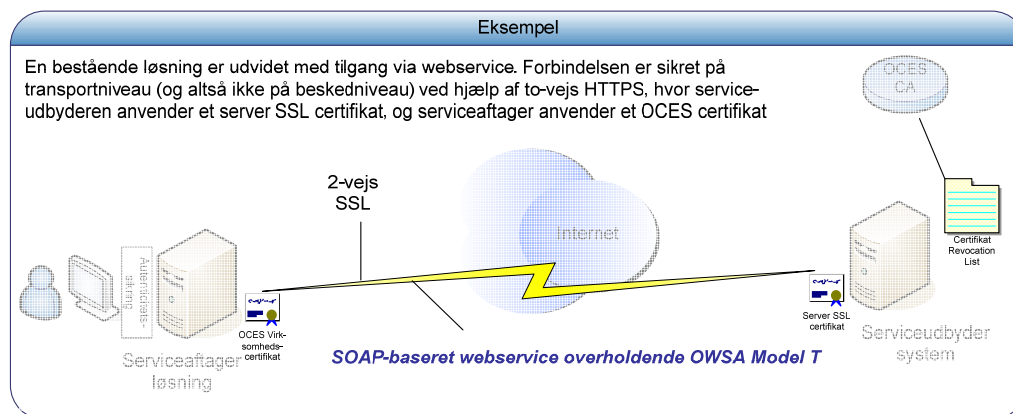
Struktur



Eksempel

Figuren herunder illustrer et eksempel hvor OWSA Model T definerer hvorledes serviceudbyder, som identificeres via et SSL servercertifikat kan tilgås sikkert af serviceaftager, som er et system, som anvender et OCES certifikat til at sikre den 2-vejs HTTPS transportforbindelse. OCES certifikatet vil typisk være et virksomhedscertifikat, men det er også muligt at anvende et borger- eller medarbejdercertifikat.

>



Deltagere

Deltagerne er

- > Serviceudbyder, som stiller data og/eller services til rådighed
- > Serviceaftager, som kan være et system eller en ekstern bruger

Derudover kan følgende implicit være deltagere i mønsteret

- > OIO Infostrukturbasen (ISB), som kan indeholde OIOXML schemaerne for de data, der udveksles
- > Det Centrale Webservice Register (CWR), som kan indeholde OIO-WSDL-definitionen for den udbudte service.

Konsekvenser

Det er muligt at etablere sikker punkt-til-punkt webservice på en ensartet måde med veletablerede teknologier.

Vejledninger og profiler

- > OWSA model T
(<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oio-web-service-arkitekturen>)
- > Vejledning for udvikling og anvendelse af OIOWSDL
(<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oio-wsdl-kontrakt-forst-udvikling-med-oioxml/?searchterm=oio-wsdl>)
- > OIO Standardkontrakt for webservices. Skabeloner til SLA-aftaler findes i kontraktens bilag
(<http://www.itst.dk/arkitektur-og-standarder/arkitektur/serviceorienteret-arkitektur/webservices/standardkontrakt-for-webservices/>)

>

Kendte anvendelser

- > Serviceaftageres forbindelse til Bygnings- og Boligregisteret (BBR)
- > ”Pension til tiden” - webservice, der kan give specifikke pensionselskaber meddelelse om personer, som tildeles førtidspension

Forbindelse med beskedbaseret sikkerhed



>

Mål

At etablere en forbindelse, hvor sikkerheden påføres på beskedniveau (modsat sikkerhed på punkt-til-punkt transportniveau)

Med sikker forbindelse menes her at serviceudbyder og -aftager kan autenticitetssikres og beskeder kan transporteres via 3. part og stadig kommunikeres med integritet og fortrolighed.

Motivation

Krav til sikkerhed og/eller fleksibilitet kan medføre behov for beskedbaseret sikkerhed.

Hvis der er krav om at integritet og/eller fortrolighed skal sikres helt frem til en given forretningsservice er transportbaseret punkt-til-punkt sikkerhed ofte utilstrækkelig, da den sikre forbindelse normalt termineres ved den første node i egen infrastruktur. Brug af beskedbaseret sikkerhed vil også give mulighed for at sende beskeder via 3. part uden at sikkerheden kompromitteres.

Kontekst

Mønsteret anvendes i forbindelse med udvikling af nye services, eller væsentlige udvidelser af eksisterende services, hvor løsningerne og værktøjerne har god understøttelse af webservice-teknologien, og hvor og udviklerne er fortrolige med værktøjernes webservice-koncepter

Løsning

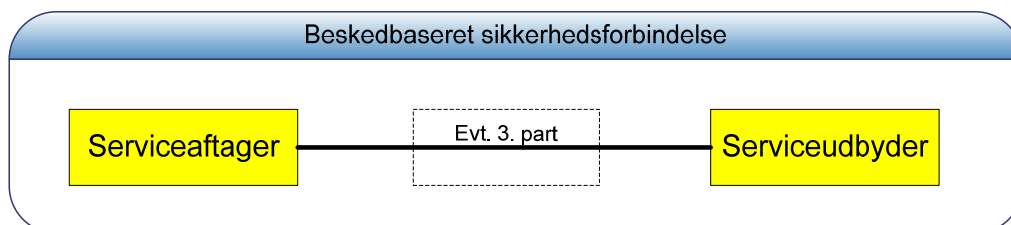
Beskedbaseret sikkerhed etableres via WS-Security-standarden i overensstemmelse med OIO Basic Security Profile V1.2, som er en profilering af WS-I Basic Security Profile 1.1.

Integritet og fortrolighed håndteres via X509 certifikater og en af følgende to typer security tokens:

- > BinarySecurityTokens med OCES Virksomheds- eller Funktionscertifikater
- > SAML assertions med "Holder of Key", hvor et X509 certifikat, som serviceudbyder stoler på bruges til at "stå inde for" serviceaftagerens certifikat.

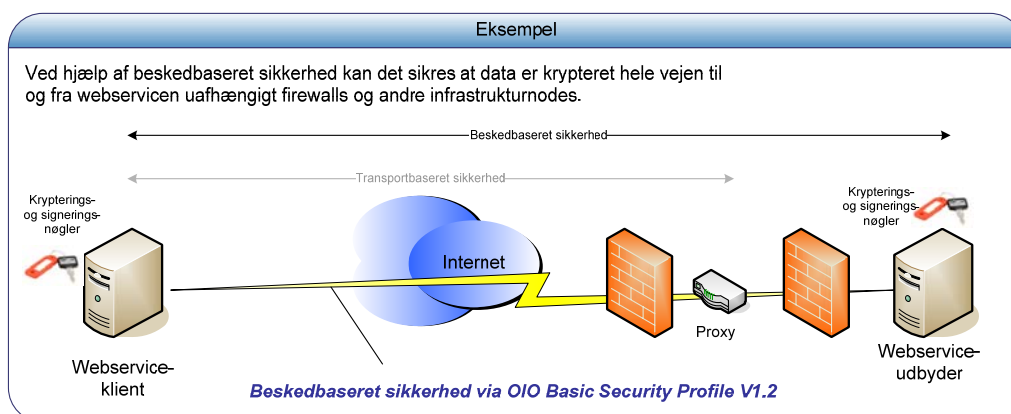
Hvis der ikke er behov for at overføre anden sikkerhedsinformation end certifikatnøgler og serviceudbyder samt serviceaftager begge findes i danske organisationer kan BinarySecurityTokens med OCES certifikater anvendes. Hvis der er behov for at overføre yderligere sikkerhedsinformation, fx roller til autorisationsbeslutninger skal SAML assertions anvendes. Ligeledes hvis serviceaftager eller serviceudbyder befinder sig i udlandet, hvor OCES certifikater ikke er tilgængelige, kan SAML assertions anvendes.

Struktur



Eksempel

Figuren herunder illustrer, hvorledes beskedbaseret sikkerhed sikrer data hele vejen til og fra webservice-udbyder..



Deltagere

Deltagerne er

- > Serviceudbyder, som er den webservice, der stiller data og/eller services til rådighed
- > Serviceaftager, som er det system eller den klient, der foretager en webservice anmodning

Derudover kan følgende implicit være deltagere i mønsteret

- > OIO Infostrukturbasen (ISB), som kan indeholde OIOXML schemaerne for de data, der udveksles
- > Det Centrale Webservice Register (CWR), som kan indeholde OIO-WSDL-definitionen for den udbudte service.

Konsekvenser

Det er muligt at etablere beskedbaseret sikkerhed på en ensartet måde, som kombinerer udnyttelse af WS-* standarder og PKI-infrastruktur.

>

En konkret implementering kræver en aftale mellem serviceaftager og serviceudbyder om service levels og de specifikke kvalitative egenskaber og gensidige forpligtigelser. Denne aftale kan formuleres som en forretningsaftale og tage udgangspunkt i OIO standardkontrakten for webservices mellem myndigheder. En af forudsætningerne for at etablere og anvende en webservice mellem myndigheder er, at der tilgodeses forpligtigelser i henhold til datatilsynets retningslinier for videregivelse af oplysninger i portaler og it-løsninger.

Vejledninger og profiler

- > OIO Basic Security Profile V1.2 - kommende
- > Vejledning for udvikling og anvendelse af OIOWSDL (<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oiowSDL-kontrakt-forst-udvikling-med-oioxml/?searchterm=oiowSDL>)
- > OIO Standardkontrakt for webservices. Skabeloner til SLA-aftaler findes i kontraktens bilag (<http://www.itst.dk/arkitektur-og-standarder/arkitektur/serviceorienteret-arkitektur/webservices/standardkontrakt-for-webservices/>)

Kendte anvendelser

- > Sikring af elektroniske fakturaer i NemHandel

Appendiks A: Relevante fælleskomponenter

>

OpenUDDI

I en serviceorienteret infrastruktur, hvor de forskellige aktører – fx. offentlige myndigheder og institutioner eller private virksomheder - ønsker at stille egne webservices til rådighed for andre og selv at kunne bruge andres webservices, er det nødvendigt at have et sted, hvor webservices kan udstilles og findes.

OpenUDDI er et register, som opfylder netop dette behov. Serviceudbydere kan let registrere deres services, så de er søgbare. Ved at slå op på en OpenUDDI-server kan andre parter lokalisere og anvende en serviceudbyders digitale services.

Anvendelse i e-handel

Et aktuelt eksempel på brug af OpenUDDI er NemHandel, hvor private virksomheder og offentlige myndigheder udveksler elektroniske handels-dokumenter. Både virksomhederne og myndighederne har i OpenUDDI registreret deres evne til at understøtte bestemte forretningsprocesser og modtage bestemte elektroniske handelsdokumenter. Deres handelspartnere kan så slå op i OpenUDDI og se, hvilke processer de understøtter.

Detaljer om OpenUDDI

OpenUDDI er en UDDI 3.0-kompatibel server implementeret i Java. Serveren understøtter gængse database- og applikationsservere og kan fungere som både master og slave i et replikeringsforhold. Serveren er afledt af Novells UDDI 3.0-server.

UDDI 3.0

- > OASIS-standard
- > Nyt abonnementsAPI, som gør det muligt at opsætte UDDI-registre i en hierarkisk struktur
- > Implementeret af HP Systinet, Oracle, BEA m.fl.

Egenskaber

- > Let at installere og afvikle
- > Beskedent ressourceforbrug
- > Høj ydelse
- > Administrativ brugergrænseflade

Implementationen

- > Udviklet under Apache 2.0 open source licens
- > Bygget på Novell UDDI 3.0
- > Administrativ brugergrænseflade udviklet i Google Web Toolkit

OpenUDDI på Softwarebørsen

<http://www.softwareborsen.dk/projekter/softwarecenter/serviceorienteret-infrastruktur/openuddi-server>

Appendix B: Referencer og links

>

- > Teknisk vejledning om sikring af digitale signaturers bevisværdi (<http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/signatur-og-systembeviser/?searchterm=systembevis>)
- > Vejledning for udvikling og anvendelse af OIOWSDL (<http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-webservices/oiowSDL-kontrakt-forst-udvikling-med-oioxml/?searchterm=oiowSDL>)
- > OIO Standardkontrakt for webservices. Skabeloner til SLA-aftaler findes i kontraktens bilag. (<http://www.itst.dk/arkitektur-og-standarder/arkitektur/serviceorienteret-arkitektur/webservices/standardkontrakt-for-webservices/>)
- > OIORASP toolkit og referenceimplementeringer. (<http://www.softwareborsen.dk/projekter/softwarecenter/serviceorienteret-infrastruktur>)

Appendix C: Proces for udvikling af indhold til implementationsmodellen

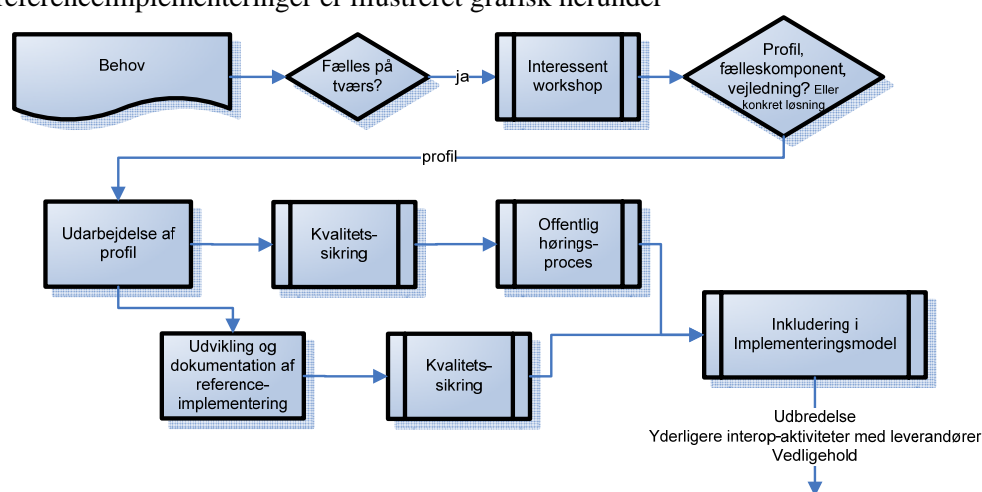
>

Dette appendiks beskriver kort processen for udvikling af indhold til implementeringsmodellen.

Gennemgangen vil fremhæve hvordan interessere kan involvere sig i arbejdet, og hvilke former for kvalitetssikring, der foretages inden resultaterne optages i implementationsmodellen.

Yderligere vil der blive diskuteret hvilke muligheder leverandører vil have for at verificere at deres løsning overholder implementationsmodellens standard-profiler

Processen for udbygning af implementeringsmodellen med standard-profiler og referenceimplementeringer er illustreret grafisk herunder



De enkelte trin, som er vist i processen herover beskrives i det følgende.

Delprocesserne for inkludering af vejledninger og fælleskomponenter i implementeringsmodellen beskrives senere i dette appendiks.

Konstatering af behov

Implementationsmodellen udbygges i forhold til den roadmap der er publiceret i ”Visioner og milepæle for national IT-infrastruktur”⁷. Udbygningen sker i nært samarbejde med myndigheder og leverandører, der har forretningsbehov, som matcher leverancerne beskrevet i roadmappen. Derudover er det også muligt at henvende sig til Center for Serviceorienteret Infrastruktur (CSI) med yderligere behov for infrastrukturelle løsninger. Ligeledes bør man henvende sig hvis man kan bidrage med infrastrukturelementer fra egne løsninger, som kan fremme udbygningen af en national it-infrastruktur. *Henvendelse til Center for Serviceorienteret Infrastruktur kan ske via email til csi@itst.dk*

⁷ [Visioner og milepæle for national IT-infrastruktur](http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/serviceorienteret-infrastruktur/visioner-og-milepele) findes online på <http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/serviceorienteret-infrastruktur/visioner-og-milepele>

Vurdering af potentialet for fælles infrastruktur

Når der indgives behov i forhold til fælles infrastruktur foretager CSI en umiddelbar vurdering af anmodningen. Dette sker primært i forhold til en konkret vurdering af om der ses potentiale for at bringe yderligere værdi til den nationale it-infrastruktur. Dette sker i dialog med relevante myndigheder og private, som CSI har partnerskabsaftaler med. Derudover vurderes også match til andre offentlige it-projektet, den fællesoffentlige digitaliseringsstrategi, etc.

Afholdelse af interessent-workshops

Hvis det vurderes at være et potentiale vil en bredere kreds af interessenter blive inddraget i at bekræfte potentialet, og i formulering af de tværgående forretningskrav som skal adresseres i en af implementeringsmodellerne.

Dette vil primært ske via workshops, som annonceres i forvejen og som er åbne for alle interesserede indenfor de lokalemæssige muligheder, etc..

Interessent-workshops annonceres på [itst.dk](http://www.itst.dk) under dette link:

<http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/implementeringsmodeller/implementeringsmodel-for-forretningservices>

Beslutning om hvorledes behov adresseres

På basis af input fra interessentworkshops afgøres hvilket ”produkt” der primært skal inkluderes i en af implementationsmodellerne. I den videre beskrivelse i denne afdeling antager vi at de givne behov bedst opfyldes med en implementerbar profil af en standard⁸, men der kunne fx også være tale om at udarbejde en vejledning, etablering af en fælleskomponent, eller noget helt fjerde. Den videre proces i forbindelse med vejledninger eller fælleskomponenter beskrives senere i dette appendiks.

Endelig er der også to andre mulige konklusioner. Det er muligt at der ikke kan findes en måde hvor opfyldelse behovet reelt vil medvirke til udbygning af den fælles it-infrastruktur. En anden konklusion kan være at behovet bedst opfyldes ved at etablere en enkelt konkret it-løsning. I dette tilfælde må der findes en organisation, som vil tage ejerskab på opfyldelse af behovet, sørge for udarbejde business case etc. – og det videre forløb forlader den her beskrevne proces i regi af CSI..

Udarbejdelse af implementerbar standard

Med afsæt i forretningskrav, brugscenarier, use cases, gennemførelse af proof of concept etc. og eksisterende standarder specificeres der de nødvendige profiler til sikring af nødvendig funktionalitet og interoperabilitet. Dette sker så vidt muligt med afsæt i internationale standarder. Disse specificeringer af hvorledes standarder anvendes til understøttelse af konkrete use case kaldes som tidligere beskrevet *profiler*.

⁸ Herunder også udvikling af en ny OIO standard, hvis der ikke findes nogen eksisterende standard, som det er relevant at profilere.

Såfremt der ikke findes relevante internationale standarder udarbejdes der nye standard/profil-specifikationer, som så vidt muligt søges indarbejdet i nye eller eksisterende internationale standardiseringsaktiviteter. Det sker for at sikre den bedste understøttelse af standarderne i it-leverandørernes produkter, og for at sikre en god proces omkring videreudvikling af de standarder, der ligger til grund for implementeringsmodellens profiler..

Kvalitetssikring af udkast til profil

Under udarbejdelsen af profilen sker der løbende en kvalitetssikring via cirkulation af udkast til interessenter, dialog med leverandører, interop-workshops, kolleger i andre lande og standardiseringsorganisationer.

Når der foreligger et færdigt udkast til profilen valideres den så vidt muligt via afprøvning med leverandørprodukter og referenceimplementeringer. Herudover reviewes profilen af en IT-Arkitekt, som ikke har deltaget i udarbejdelsen af profilen, men som har god viden på området.

Offentlig høring

Efter kvalitetssikring af det færdige udkast sendes profilen i 30 dages offentlig OIO-høring.

Indsendte høringsvar offentliggøres på høringsportalen. Der udarbejdes et notat over de indsendte høringsvar med angivelse af forslag til evt. ændringer til profilen. Høringsresultatet behandles derefter i [OIO-komiteen]. Hvis komiteen godkender standard-profilen inkluderes den i OIO-kataloget og den relevante implementationsmodel.

Alt materiale, som CSI sender i offentlig høring, såvel som de indkomne høringsvar, publiceres på høringsportalen:

<http://borger.dk/forside/lovgivning/hoeringsportalen>

Hvis du ønsker at modtage email-notifikation når nye OIO-standarder sendes i høring, kan du bede om at komme på høringslisten ved sende en email til: oiostandarder@itst.dk

Udvikling og dokumentation af referenceimplementering

Sideløbende med arbejdet med udvikling af profil udvikles der en eller flere referenceimplementeringer, som kan hjælpe udvikleren til at forstå hvorledes den givne standard-profil konkret implementeres, og som også kan anvendes til at teste op imod under udviklingsarbejdet.

Afhængigt af behov og muligheder vil referenceimplementeringen indeholde en dokumenteret værktøjskasse (toolkit) som udvikleren kan anvende til implementation af profilen i egen løsning. Referenceimplementeringen vil evt. blive implementeret i flere varianter hvis det skønnes vigtigt i forhold til platformsneutralitet, fx både til Java- og .Net-plattformen.

Kvalitetssikring af referenceimplementering

Før en referenceimplementering frigives til almindelig anvendelse kvalitetssikres implementeringens korrekthed i forhold til den givne standard-profil, omfang af

>

dokumentation og generel robusthed af koden. Kvalitetssikringen foregår via en eller flere af de følgende aktiviteter:

kodereview af uafhængig IT-Arkitekt, funktionstest, interoperabilitetstest. I dokumentationen til referenceimplementeringen angives det hvilken form for kvalitetssikring den har gennemgået. Herefter er referenceimplementeringen parat til at indgå i implementationsmodellens indhold.

Inkludering i implementationsmodel

En godkendt profil inkluderes i implementationsmodellen ved at den publiceres på www.itst.dk, som en del af implementationsmodellen. Dokumentationen af implementationsmodellen opdateres, så der henvises til profilen fra de relevante mønstre i modellen.

En referenceimplementering inkluderes i implementationsmodellen ved at der referes til den fra implementationsmodellen på www.itst.dk. Med mindre andre hensyn spiller ind placeres referenceimplementeringen på softwarebørsen: softwareborsen.dk. Herefter opdateres dokumentationen af implementationsmodellen med henvisninger til hvor referenceimplementeringen og evt. tilhørende toolkit og dokumentation kan hentes.

Nyt indhold i implementationsmodellen publiceres under dette link:

<http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/implementeringsmodeller/implementeringsmodel-for-forretningsservices>

Opfølgende aktiviteter

Efter tilføjelse af et produkt (standard-profil, referenceimplementation, etc.) til implementationsmodellen foretages der for de fleste produkter en række opfølgende aktiviteter med henblik på at øge udbredelsen af produkterne. Det kan inkludere kommunikation, afholdelse af uddannelse/workshops, særlig støtte til ”first movers”-projekter med mere.

Verifikation af overholdelse

Der vil også blive beskrevet hvorledes leverandører kan verificere at deres produkter overholder en profil i en implementationsmodel. Dette vil så vidt muligt ske via konkret aftestning af leverandørens produkt. Dette kan ske på flere måder, herunder

- > Leverandøren tester sit eget produkt i samspil med en referenceimplementering, og foretager en egenvurdering af i hvor høj grad standard-profilen overholdes.
- > Leverandøren deltager i en interoperabilitetsbegivenhed, hvor det dokumenteres hvor mange testcases, der er gennemført succesfuldt med leverandørens produkt.
- > Leverandøren deltager med sit produkt i et formelt testprogram, hvor der er en 3. part som står inde for at leverandørens produkt har bevist interoperabilitet og er funktionsmæssigt komplet.

Dette var kort trinene i processen med at udvikle en profil med tilhørende referenceimplementering til implementationsmodellen.

>

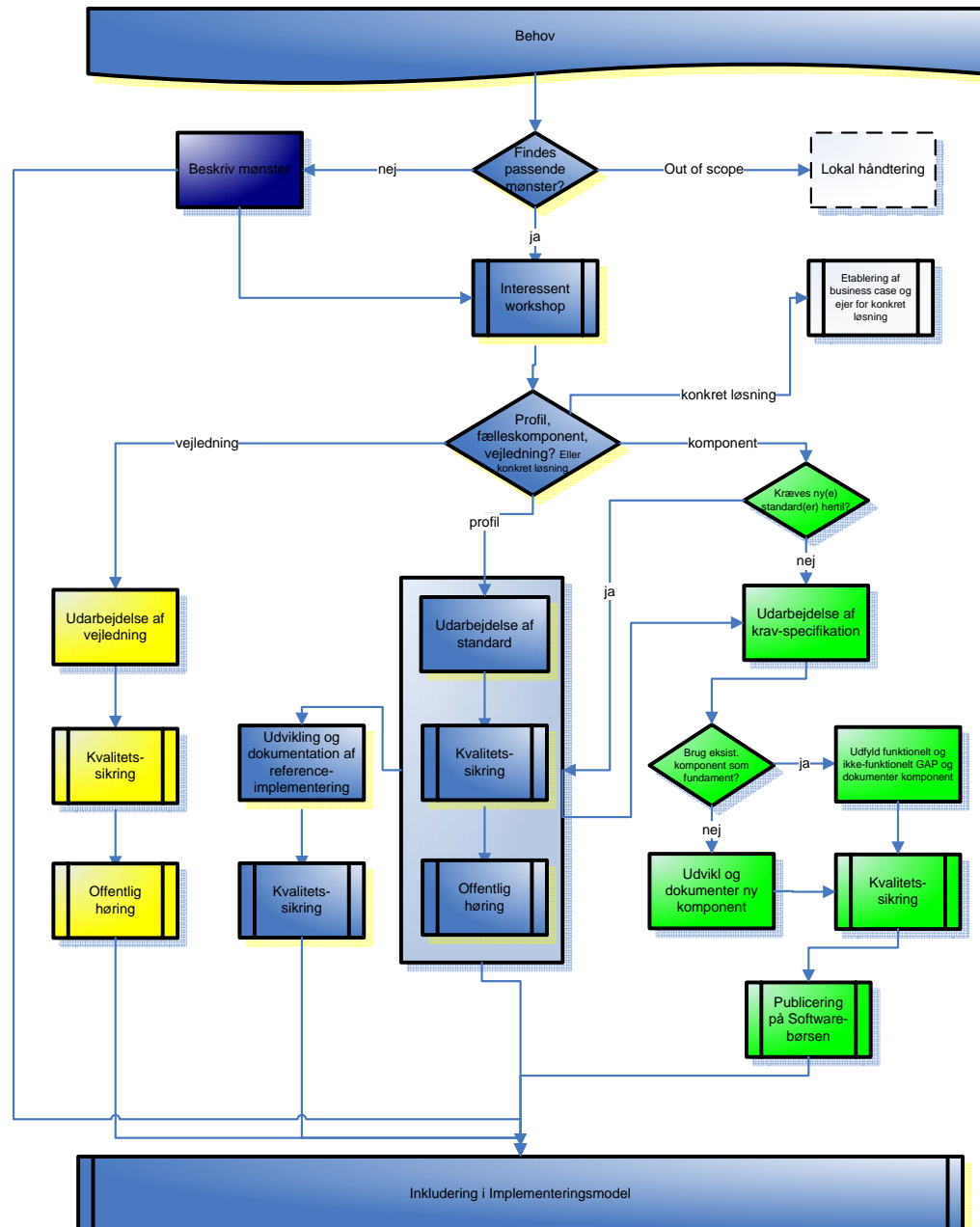
Andre produkter kan også indgå i implementationsmodellen. I det følgende beskrives processen fra behov til inkludering i implementationsmodel for vejledninger, fælleskomponenter og yderligere integrationsmønstre.

Udvikling af vejledninger, fælleskomponenter og yderligere integrationsmønstre

I nedenstående figur er processen, som vi allerede har gennemgået, udvidet med yderligere ”produkter”. De dele af processen, som vedrører profiler og referenceimplementeringer består af de blå figurer. Herudover er der tilføjet andre trin vedrørende yderligere mønstre til implementationsmodellen (mørkeblå figur), vejledninger, (gule figurer) og fælleskomponenter (grønne figurer)

De specielle ting vedrørende de ekstra produkter beskrives kort i det følgende.

>



Yderligere mønstre til implementationsmodellen

Implementationsmodellen indeholder mønstre, som matcher de kendte behov og krav til fælles infrastruktur for forretningsservices. I forbindelse med der opstår yderligere behov, kan det vise sig at implementationsmodellen ikke har noget mønster, som matcher en løsning på det nye behov. I dette tilfælde beskriver CSI et nyt mønster, som inkluderes i implementationsmodellen samtidig med at det valideres på en interessent-workshop.

Vejledninger

En mulig konklusion fra en interessentworkshop kan være at der måske ikke direkte er behov for en standard-profil, men at det stadig giver værdi med en vejledning indenfor et givent område.

I så tilfælde udarbejder CSI en vejledning – gerne i samarbejde med den part, der havde det konkrete behov. Vejledningen kvalitetssikres via review hos et udvalg af væsentlige interessenter. Herefter sendes vejledningen i offentlig høring, og endelig inkluderes vejledningen i relevante mønstre i implementationsmodellen

Fælleskomponenter

Et andet resultat af behovsaflæringen kan være at der viser behov for en konkret funktionel komponent, som kan anvendes i flere it-løsninger (fx frem for etablering af en central løsning). Det kan være en fælleskomponent, som kan anvendes for sig selv – eller det kan være en komponent, som nemt kan integreres med anden infrastruktur/ en forretningsløsning. Hvis muligt udvikles fælleskomponenten ved at videreudvikle en specifik løsning til en mere generel komponent. Der kan også blive tale om videreudvikling af en open source komponent med basal funktionalitet – og endeligt kan der blive tale om at udvikle en fælleskomponent fra bunden. I alle tilfælde udarbejdes der først en overordnet kravspecifikation.

En ny komponent udvikles på basis af kravspecifikationen. Hvis fælleskomponenten skal baseres på en eksisterende løsning videreudvikles der på de områder hvor der er mangler i forhold til ønsket funktionalitet.

Fælleskomponenten gennemgår ligesom referenceimplementeringerne en kvalitetsikring med kodereview, aftenstning, mm. Herefter frigives den som en Open Source komponent på Softwarebørsen og inkluderes i Implementationsmodellen.

Open Source fælleskomponenter publiceres på Softwarebørsen:
[http:// softwareborsen.dk](http://softwareborsen.dk)

Hermed afsluttes gennemgangen af proces for udvikling af indhold til implementationsmodellen.

Aktuel status på indhold i implementationsmodellen findes på
<http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/implementeringsmodeller/implementeringsmodel-for-forretningservices>



Implementeringsmodel for forretningsservices

Målet med denne "implementeringsmodel for forretningsservices" er at bistå offentlige myndigheder og private virksomheder med deres valg af webservice-profil i forbindelse med eksponering af services og registre samt udveksling af forretningsdokumenter. En webservice-profil er en specialisering af en webservice-standard i forhold til et givet formål.

Center for Serviceorienteret Infrastruktur(CSI) er en del af IT- og Telestyrelsen og er med til at skabe Danmarks nationale e-infrastruktur, som er fundamentet for digitalisering i både den offentlige og private sektor.

