

Indholdsfortegnelse

HVOR KAN MAN ANVENDE OIO SERVICEORIENTERET INFRASTRUKTUR?.....	1
ADRESSERING AF SERVICES.....	2
INTEROPERABILITETSPROFIL.....	2

Til det offentlige stilles der krav om, at indberetninger skal kunne ske elektronisk, og at myndighedernes data og services kan tilgås via veldefinerede grænsesnit i et miljø, hvor sikkerhed og pålidelighed er i højsædet.

Denne udvikling indebærer en risiko for, at der ikke sker en koordination i forhold til anvendelsen af netværksinfrastruktur og tekniske standarder med øgede omkostninger og besværligere integration til følge.

UDGANGSPUNKTET FOR OIO SERVICEORIENTERET INFRASTRUKTUR HAR DERFOR VÆRET:¹

- At samle de forretningsmæssige krav til udveksling af forretningsdokumenter via internettet.
- At etablere en infrastruktur der for dataudveksling som opfylder de stillede krav til sikkerhed og pålidelighed.

Udviklingen er sket i tæt dialog med centrale offentlige myndigheder og private virksomheder for at sikre, at den infrastruktur, der etableres, ikke alene skaber fælles rammebetingelser for dataudveksling i den offentlige sektor, men at den giver grobund for vækst og muligheder i den private sektor.

ITST har med initiativet ”OIO Serviceorienteret Infrastruktur” (OIOSI) lagt byggestenene til en national webservice infrastruktur, som med tiden kan kombineres med andre services til understøttelse af brugerstyring og orkestrering af individuelle services i sammenhængende forretningsprocesser.

HVOR KAN MAN ANVENDE OIO SERVICEORIENTERET INFRASTRUKTUR?

OIO Serviceorienteret Infrastruktur er et sæt af byggeklodser, der kan anvendes i alle typer projekter, der kræver udveksling af data på en sikker og pålidelig måde mellem myndigheder, applikationer eller services. Fx kan infrastrukturen anvendes som fundament til:

1. Sikker og pålidelig indberetning af data direkte fra virksomheders ERP-systemer til offentlige myndigheder.
2. Sikker og pålidelig udveksling af forretningsdokumenter mellem myndigheder, borgere og virksomheder.
3. Eksponering af data og services fra myndigheder og private virksomheder.
4. Udveksling af forretningsdokumenter på tværs af forskellige netværksinfrastrukturer.

¹www.oio.dk

Fx fra OIOSI til en VANS-infrastruktur eller en bank-infrastruktur eller over landegrænser til andre nationale infrastruktur-løsninger.

5. Udveksling af forretningsdokumenter via en service hos en betroet tredjepart, som fx kan varetage format-konvertering.
6. Samling og orkestrering af services til nye anvendelser i en service bus.

Uanset hvor man anvender OIO serviceorienteret kataloget, og at løsningerne Infrastruktur, sikrer brugen af de fælles offentlige kan overholde lovgivningen og standardiserede byggeklodser, at de løsninger, mht. sikker og fortrolig man udvikler, kan snakke sammen på tværs og i udveksling af personfølsomme øvrigt er i overensstemmelse med de fælles oplysninger. offentlige standarder, som er publiceret i OIO-

Tekst 1: daadf

Tekst 2: Dette er en test er tekstboks.. Sådan!!!

ADRESSERING AF SERVICES

Adresseringsmekanismen er baseret på et register, som overholder den internationale standard UDDI (Universal Discovery, Description and Integration). UDDI-registret udstiller en række standardiserede grænseflader via web services, som tillader, at udbydere af services (fx en offentlige myndighed som har etableret en service til elektronisk indberetning) kan informere brugerne af servicen (serviceaftagere) om, hvor og hvordan disse services kan tilgås.

Visionen om anvendelse af adresseringsmekanismer til såkaldte 'dynamisk binding' mellem uafhængige serviceudbydere og serviceaftagere er ikke ny, og inden for web serviceområdet har UDDI-registre kun vundet begrænset udbredelse som bindeled for services på tværs af organisationer.

Udfordringerne ved anvendelsen af UDDI-registre i web service sammenhæng kan tilskrives en række faktorer, som netop imødegås i OIOSI. For det første vil UDDI-registret i OIOSI hovedsageligt blive anvendt til simple opslag med få parametre i stil med "giv mig adresseoplysninger for services til indberetning af sygedagpengerefusion for den offentlige myndighed med EAN-lokationsnummer..". For det andet vil anvendelsen af web service standarder blive samlet i profiler; de såkaldte interoperabilitetsprofiler.

INTEROPERABILITETSPROFIL

En interoperabilitetsprofil beskriver meget detaljeret, hvilket standarder der skal anvendes i udvekslingen mellem en serviceudbyder og en serviceaftager. På de områder, hvor standarderne lægger op til valg, vil profilen reducere valgmulighederne til et minimum. Inden for rammen af OIOSI vil der blive udviklet et begrænset antal profiler, som hver især understøtter forskellige forretningsmæssige krav. Den første profil, som udvikles, kaldes OIO-RASP, hvor RASP står for "Reliable Asynchronous Secure Profile". OIO-RASP bygger på den såkaldte WS*-stak af standarder, som udvikles i regi af OASIS (Organization for the Advancement of Structured Information Standards). WS*-stakken bliver yderligere profileret i en anden international organisation, WS-I (Web Service Interoperability), der arbejder for at sikre interoperabilitet på tværs af forskellige leverandørers platforme. OIO-RASP bygger på WS-I profiler, hvor det overhovedet er muligt og gør brug af en stribe undetliggende WS* standarder: SOAP 1.1, WSDL 1.1, UDDI 2.0, XML 1.0, XML Schema 1.0, WS-Security og WS-Reliablemessaging. OIO-RASP beskriver med andre i detaljer, hvordan standarderne skal benyttes i sammenhæng, således at understøttelsen af profilen gøres lettest mulig.

Med hensyn til valg af underliggende protokoller afviger OIO-RASP på et enkelt punkt fra den gængse http binding for web services. Da det er et forretningsmæssigt krav, at også små organisationer (fx enkeltmandsvirksomheder) skal kunne modtage og afsende elektroniske forretningsdokumenter 24 timer i døgnet året rundt, har det vist sig formålstjenligt også at understøtte SMTP/POP3-standarderne for elektronisk post. Profilen udnytter, at de fleste internet-abonement giver adgang til en SMTP-server, hvor virksomheden kan modtage elektronisk post døgnet rundt.

SIKKERHED

Sikkerheden i OIOSI er bygget op omkring en PKI-infrastruktur baseret på den offentlige OCES-standard (Offentligt Certifikat til Elektronisk Service). En serviceudbyders offentlige nøgle benyttes til at kryptere meddelelser, som sendes fra serviceaftagere, således at vedkommende ikke kan læse indholdet af meddelelsen. Inden afsendelse signerer serviceaftageren på tilsvarende vis meddelelsen og vedhæfter et security token med sit certifikat. Derved kan serviceudbyderen autentificere serviceaftageren og ved at validere signaturen kan det sikres, at meddelelsen ikke er blevet kompromitteret under forsendelsen. Politikker formuleret i OIO-RASP beskriver, hvordan serviceudbyderen skal reagere i tilfælde af, at en meddelelse er blevet kompromitteret, eller at signeringen er sket med et invalidd certifikat.



MILEPÆLE OG KURSER

- 15. September 2006: Teknisk pilotprojekt for de it-leverandører og institutioner, der ønsker at afprøve webservice infrastrukturen.
- 12.-17. november 2006: International UBL konference i København, der også dækker infrastruktur (<http://www.ublconference.com>).
- 1. februar 2007: Første pilot med involvering af både it-leverandører og virksomheder starter. Denne pilot gennemføres i samarbejde med it-leverandører og brancheorganisationer. Det vil være muligt for virksomheder at tilmelde sig piloten
- 1. juli 2007: Bred lancering for den private sektor af OIO Serviceorienteret Infrastruktur til brug for udveksling af e-handelsdokumenter, baseret på OIOUBL.

Testtabel

Denne	Tabel	Er	Bare	En	Test
Af	Funktionalitet	Så	Den	Betyder	Ikke
Noget	Som	Helst	Og	Kan	Derfor
Ignorerer	Hvis	Man	Ikke	Gider At	
Kigge	Alle	Disse	Irraterende	Felter	Igennem
Når	De	Nu	Ikke	Betyder	Noget

Testregneark

Testnr/test	X2	X4	X6	X8	X10
1	2	4	6	8	10
2	4	8	12	16	20
3	6	12	18	24	30
4	8	16	24	32	40
5	10	20	30	40	50
6	12	24	36	48	60
7	14	28	42	56	70
8	16	32	48	64	80
9	18	36	54	72	90
10	20	40	60	80	100

Testtegning