Vejledning om anvendelse af obligatoriske, åbne standarder for software i det offentlige.

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

>

Vejledning om anvendelse af obligatoriske, åbne standarder for software i det offentlige

Udgivet af:
Videnskabsministeriet

Ministeriet for Videnskab, Teknologi og Udvikling
Bredgade 43
1260 København K

Telefon: 3392 9700
Fax: 3332 3501

Publikationen udleveres gratis
Så længe lager haves, ved henvendelse til:

IT- og Telestyrelsen.

Publikationen kan også hentes på Videnskabsministeriets Hjemmeside: http://www.vtu.dk
ISBN (internet):

Tryk:

Oplag:
ISBN:

>

Vejledning om anvendelse af obligatoriske, åbne standarder for software i det offentlige

Ministeriet for Videnskab, Teknologi og Udvikling
Oktober 2007

Indhold >

Obligatoriske, åbne standarder

>

Den 1. januar 2008 vil en række åbne standarder blive obligatoriske at anvende for offentlige myndigheder ved fremtidige indkøb af software og it-løsninger.

For offentlige myndigheder betyder det, at man skal sikre sig, at fremtidige it-løsninger er baseret på, eller understøtter, disse obligatoriske, åbne standarder, hvis standarderne er relevante for it-løsningen. For alle de obligatoriske, åbne standarder gælder, at den enkelte myndighed ved eventuelle merudgifter eller for den pågældende myndighed it-sikkerhedsmæssige hensyn kan undlade at anvende de obligatoriske standarder

Anvendelse af obligatoriske, åbne standarder medfører ikke et forbud mod anvendelse af andre standarder end de obligatoriske, åbne standarder. It-løsninger må således gerne kunne anvende andre standarder end de obligatoriske, åbne standarder, så længe løsningerne også understøtter anvendelsen af de relevante obligatoriske, åbne standarder.

Der er ingen krav om at anvende bestemte typer eller fabrikater af software, og der er ingen krav om, at de pågældende formater anvendes som det interne format i software.

Ved offentlige myndigheder forstås kommunale og regionale forvaltninger, statslige departementer, styrelser og direktorater.

Ved obligatoriske, åbne standarder forstås udvalgte og navngivne standarder, som er vurderet hensigtsmæssige for anvendelse i den offentlige sektor.

Denne vejledning baserer sig på nedenstående aftale, der er indgået mellem regeringen, KL og Danske Regioner

Regeringsbeslutning og aftale om anvendelse af åbne standarder for software i det offentlige

Den 2. juni 2006 vedtog et enigt Folketing folketingsbeslutning B 103 om anvendelse af åbne standarder for software i det offentlige. Folketingsbeslutningen pålægger regeringen at sikre, at det offentliges brug af informationsteknologi, herunder brug af software, er baseret på åbne standarder. Et flertal af partierne har lagt til grund, at anvendelsen af åbne, obligatoriske standarder ikke må medføre øgede udgifter for det offentlige.

11. august 2006 offentliggjordes rapporten ”Virkemidler til fremme af interoperabilitet gennem fælles, åbne standarder”. Bag rapporten stod Videnskabsministeriet, Finansministeriet, KL og Danske Regioner. Rapporten lagde en fællesoffentlig basis for hvordan anvendelsen af obligatoriske, åbne standarder kunne gennemføres. Herunder at anvendelsen blev gennemført ved en regeringsbeslutning og en aftale med de kommunale parter.

I februar 2007 sendte IT- og Telestyrelsen rapporten ”Anvendelse af åbne standarder for software i det offentlige” i høring. Denne rapport anbefaler, at syv software-standarder gøres obligatoriske pr. 1. januar 2008.

>

Høringssvarene var overvejende positive, og videnskabsministeren opnåede efterfølgende en politisk enighed om en køreplan for implementering af anvendelse af obligatoriske, åbne standarder for software i det offentlige.

Obligatoriske, åbne standarder
Indførelsen af åbne standarder skal, uden at det medfører øgede udgifter for det offentlige, fremme et konkurrencepræget marked for software og medvirke til, at offentlige it-systemer uanset valg af software kan udveksle informationer på tværs.

For hvert potentielt set obligatoriske sæt af åbne standarder gennemføres en økonomisk konsekvensvurdering. Vurderingen sikrer, at indførelsen af den enkelte standard er samfundsøkonomisk hensigtsmæssig.

At en standard er åben indebærer, at:

- standarden skal være fuldstændigt dokumenteret og offentligt tilgængelig,
- standarden skal være frit implementérbar uden økonomiske, politiske eller juridiske begrænsninger på implementering og anvendelse, hverken nu eller i fremtiden, og
- standarden skal være standardiseret og vedligeholdt i et åbent forum via en åben proces (standardiseringsorganisation).

De første syv sæt af obligatoriske, åbne standarder træder i kraft fra den 1. januar 2008. Det drejer det sig om følgende sæt af standarder:

- Standarder for dataudveksling mellem offentlige myndigheder (OIOXML)
- Standarder til elektronisk sags- og dokumenthåndtering (FESD)
- Standarder til elektroniske indkøb i det offentlige (OIOUBL)
- Standarder for digital signatur (OCES)
- Standarder for offentlige netsteder / hjemmesider og tilgængelighed
- Standarder for it-sikkerhed (DS484 - kun for staten)
- Standarder for dokumentudveksling (ODF/OOXML)

Vedrørende standarder for dokumentudveksling eksisterer der i dag to åbne væsentlige standarder for disse formater på markedet: ODF og OOXML. Begge standarder er dog stadig relativt umodne, og der mangler konkrete erfaringer med deres anvendelse i praksis. Derfor er de økonomiske konsekvenser ved at indføre dem vanskelige at estimere og baseret på et stort skønselement. Samme erkendelse er man ligeledes nået frem til i andre europæiske lande, der står over for lignende beslutninger.

Derfor igangsættes følgende implementering:

- Den 1. januar 2008 skal alle offentlige myndigheder kunne modtage tekstbehandlingsdokumenter fra borgere, virksomheder og andre myndigheder i to formater: OOXML og ODF.
- Pr. 1. januar 2008 bliver OOXML og ODF obligatoriske standarder for offentlige myndigheder. Løsninger, der indkøbes efter 1. januar 2008, skal understøtte mindst en af disse åbne standarder og kunne modtage tekstbehandlingsdokumenter i begge formater, evt. ved brug af tilføjelsesprogrammer (plug-ins).

>

- Om ODF og /eller OOXML skal være obligatoriske efter 1. juli 2009 afgøres efter en vurdering af en uafhængig tredjepart.

Anvendelse af obligatoriske, åbne standarder
Kravet om anvendelse af obligatoriske, åbne standarder gælder alene for nye it-løsninger.

For anvendelsen af obligatoriske, åbne standarder gælder, at den enkelte myndighed ved eventuelle merudgifter eller andre uhensigtsmæssigheder, herunder i forhold til den pågældende myndigheds it-sikkerhedsmæssige hensyn, kan undlade at anvende de obligatoriske standarder.

De nærmere retningslinjer, herunder hvordan en undladelse kan begrundes, fastsættes i de generelle vejledninger, der udarbejdes på baggrund af implementeringen af obligatoriske, åbne standarder.

Anvendelse af obligatoriske, åbne standarder

>

Det er i anvendelsen af standarder, at deres værdi realiseres. Det er samtidigt vigtigt at undgå, at den enkelte myndighed tvinges til at foretage uhensigtsmæssige valg og fremskynde indkøb og udvikling i forhold til det administrative behov, eller at de afstår fra at etablere en it-løsning, fordi det bliver for dyrt eller besværligt. Af denne grund fastsættes en række undtagelsesbestemmelser for kravet om anvendelse af obligatoriske, åbne standarder.

Fra 1. januar 2008 forudsættes det, at al offentlig nyudvikling udarbejdes med obligatoriske, åbne standarder som en del af grundlaget.

Det vil sige, at myndigheder, der gennemfører udbud og udviklingsprojekter inden for de områder, hvor der er defineret obligatoriske åbne standarder, inddrager disse som en del af grundlaget for projektet.

Ved nye løsninger forstås nyindkøb og nyudvikling, samt videreudvikling og opgradering af software, med mindre dette foregår som en del af en allerede indgået aftale.

Myndigheder kan i forbindelse med udbud og udviklingsprojekter undtage sig selv fra reglerne om at anvende obligatoriske, åbne standarder, hvis myndigheden dermed tvinges til en løsning, der enten:

> er væsentligt fordyrende i forhold til anvendelse af andre standarder,

> svækker sikkerhedsniveauet væsentligt i forhold til anvendelse af andre standarder,

> medfører væsentlig funktionel forringelse, der er direkte forårsaget af, at den er baseret på de obligatoriske, åbne standarder,

> øger implementeringstiden markant,

> medfører konflikt med standarder, der på grund af internationale forpligtelser er gældende inden for enkeltområder.

Såfremt et eller flere af ovenstående punkter gør sig gældende, kan den givne myndighed vælge at fravige konkrete obligatoriske, åbne standarder i den givne løsning.

Vurderes det, at kravet skal fraviges, giver det anledning til en såkaldt *forklaring.* Med dette skal forstås, at der skal udarbejdes en forklaring fra den givne myndighed, der redegør nærmere for de omstændigheder, der i situationen ligger bag en fravigelse af kravet om overholdelse af det obligatoriske sæt af åbne standarder.

Krav og forudsætninger for fravigelse herfra udgør tilsammen en *følg eller forklar*-model.

>

Hvilke standarder er relevante?

Den enkelte myndighed bør indlede vurderingen af spørgsmålet om anvendelse af obligatoriske standarder i forbindelse med foranalysefasen i et givent it-projekt. Vurderingen består i en identifikation af, hvilke af de obligatoriske, åbne standarder, der har relevans inden for det område, som systemløsningen dækker.

Egenudvikling

Hvor myndigheden besidder størstedelen af projektledelseskompetencen, bør vurderingen af eventuelle negative konsekvenser ved anvendelse af obligatoriske, åbne standarder være gennemført inden projektets igangsættelse endeligt godkendes.

Indkøb og udbud

Ved indkøb med eller uden et udbud, bør vurderingen indgå i eller som bilag til kravspecifikationen, idet den offentlige myndighed samtidig adresserer en entydig forventning om, at leverandørens løsningsbeskrivelse tager afsæt i et sæt obligatoriske åbne standarder, såfremt disse er relevante at anvende inden for det givne løsningsområde.

I forbindelse med opstilling af disse krav om anvendelse af standarder skal leverandøren gøres opmærksom på baggrunden herfor, det vil sige de hovedprincipper, der ligger bag *følg eller forklar*. Leverandøren bør tilsvarende informeres om, hvilke standarder der på et givent tidspunkt er obligatoriske. Endelig skal leverandøren gøres opmærksom på, at kravet kan afviges på baggrund af de opstillede undtagelsesbestemmelser. Såfremt en eller flere af årsagerne til fravigelse gør sig gældende, og leverandøren vurderer, at det bør have indflydelse på løsningsbeskrivelsen, skal der udarbejdes en nærmere begrundelse herfor.

Myndigheden præsenteres således for en løsningsbeskrivelse fra leverandøren, der forholder sig til, hvorvidt åbne obligatoriske standarder er relevante at anvende i den givne kontekst, og om disse i så fald kan overholdes eller falder ind under undtagelsesbestemmelserne. I tilfælde af, at den obligatoriske standard anvendes, angives dette af leverandøren. I tilfælde af, at der undtages fra anvendelsen, vil de nærmere omstændigheder og dokumentationen herfor skulle angives.

Hvordan ordregivende myndigheder inddrager obligatoriske, åbne standarder i sit udbudsmateriale

For at sikre at ordregivende myndigheder inddrager obligatoriske, åbne standarder ved køb af it-løsninger foreslås det, at udbudsmaterialer udformes på følgende måde:

1. Giv mulighed for, at tilbudsgiver kan afgive alternative tilbud, hvis tilbudsgiver vurderer, at det ikke er hensigtsmæssigt for ordregivende myndighed at basere sig på de obligatoriske, åbne standarder i den konkrete sammenhæng. Hermed gives tilbudsgiverne mulighed for at afgive to typer tilbud:
   - et tilbud der baseres på/understøtter obligatoriske, åbne standarder
   - et tilbud der ikke baseres på/understøtter obligatoriske, åbne standarder.

2. Muligheden for at afgive alternative tilbud skal være angivet i

>

udbudsbekendtgørelsen. Det er et krav at tildelingen af kontrakten sker på grundlag af tildelingskriteriet "det økonomisk mest fordelagtige tilbud".

3. Opstil krav til it-løsningen i udbudsgrundlaget.

4. Angiv hvilke hvilke af disse krav der er minimumskrav d.v.s. krav som alle tilbud skal opfylde for at være konditionsmæssige. Disse minimumskrav kan vedrøre sikkerhed, tidsrammer og funktionalitet. Også internationale forpligtelser som it-løsningen skal overholde angives som minimumskrav

Når den ordregivende myndighed modtager tilbud, kan myndigheden vælge det økonomisk mest fordelagtige tilbud blandt både de tilbud der opfylder alle krav i udbudsgrundlaget eller de tilbud der har kommet med alternative løsningsforslag.

I dette valg indgår også en vurdering af, eventuelle negative konsekvenser der kan følge af at vælge en it-løsning, der baseres på/understøtter obligatoriske, åbne standarder. Disse negative konsekvenser gennemgås nærmere nedenfor.

Begrundelse for anvendelse af undtagelsesbestemmelser

Der er opstillet en række kriterier for, hvornår en myndighed kan undtages fra reglerne om at anvende obligatoriske åbne standarder på et konkret område. I disse tilfælde skal der foretages en uddybende begrundelse for behovet for denne undtagelse.

Uanset om redegørelsen udarbejdes af den offentlige myndighed, af den private leverandør eller hvis det sker i fællesskab, bør begrundelsen så vidt muligt indeholde følgende oplysninger.

Øgede udviklingsomkostninger:

> Skønnede meromkostninger, både absolut i forhold til den samlede anskaffelsessum.

> Der angives eventuelle negative konsekvenser for anden myndighed ved, at løsning ikke anvender obligatoriske standarder.

Svækket sikkerhedsniveau:

> Det angives, hvorfor det vurderes, at sikkerhedsniveauet svækkes væsentligt.

Funktionel forringelse:

> Det begrundes, hvorfor der forventes en funktionel forringelse som følge af anvendelse af obligatoriske åbne standarder, herunder hvorvidt det skyldes et eller flere af følgende forhold:
    - Manglende mulighed for integration
    - Konflikt med andre allerede anvendte standarder, der ikke kan fraviges

>

Væsentlig forsinkelse:

> Vurdering af hvor meget projektet forsinkes, og evt. hvilke afledte konsekvenser det giver.

Konflikt med sektorfastsatte standarder:

> Hvis undtagelsen begrundes med henvisning til konflikt med standarder, der på grund af internationale forpligtelser er gældende inden for enkeltområder, vedlægges henvisning til sektorbeslutning.

Offentliggørelse af anvendelse af undtagelsesbestemmelserne

Ved nye løsninger, hvor den tekniske anskaffelse har samlede omkostninger, der overstiger EU's udbudsgrænse, skal de udarbejdede begrundelser for anvendelse af undtagelsesbestemmelserne offentliggøres. Dette kan ske ved

- at myndigheden sender begrundelserne til IT- og Telestyrelsen i forbindelse med underskrivelse af kontrakten, hvorefter IT- og Telestyrelsen vil sørge for offentliggørelse,
- at offentliggøre begrundelserne på myndighedens egen hjemmeside eller
- at offentliggøre begrundelserne i forbindelse med regnskabsaflæggelse.

Nye løsninger, hvis samlede omkostninger ligger under denne grænse, skal ligeledes anvende obligatoriske åbne standarder, medmindre de falder ind under undtagelsesbestemmelserne. Disse løsninger er dog ikke underlagt kravet om offentliggørelse af eventuelle undtagelsesbestemmelser. Dog opfordres myndighederne også at offentliggøre disse

Krav om offentliggørelse bringes ikke i anvendelse for systemer, der er omfattet af Statsministeriets sikkerhedscirkulære.

Sæt af obligatoriske, åbne standarder

>

Det er først, når en standard anvendes, og ofte når den anvendes i tilknytning til andre standarder, at dens potentielle værdi i forhold til at sikre interoperabilitet for alvor kan realiseres. Standarder skal derfor betragtes i en anvendelseskontekst. En anvendelseskontekst kan for eksempel være dataudveksling mellem systemer, tværgående brugerstyring eller borgeres adgang til offentlig information via internettet.

For hver af sådanne anvendelseskontekster vil der typisk være mere end én relevant standard. Man kan derfor tale om, at der vil være et sæt af standarder knyttet til hver kontekst.

Videnskabsministeren og Folketingets it-ordførere er blevet enige om en køreplan for anvendelsen af obligatoriske åbne standarder, hvor syv sæt af standarder bliver obligatoriske fra 1. januar 2008

De syv sæt af standarder er:

- Standarder for dataudveksling mellem offentlige myndigheder (OIOXML)
- Standarder til elektronisk sags- og dokumenthåndtering (FESD)
- Standarder til elektroniske indkøb i det offentlige (OIOUBL)
- Standarder for digital signatur (OCES)
- Standarder for offentlige netsteder / hjemmesider og tilgængelighed (HTML/XHTML, CSS og WCAG)
- Standarder for it-sikkerhed (DS-484)
- Standarder for dokumentudveksling (ODF/OOXML)

De følgende sider beskriver hvert enkelt sæt af standarder nærmere.

Standarder for dataudveksling mellem offentlige myndigheder (OIOXML) >

En forudsætning for en effektiv digital forvaltning er, at dataudveksling mellem systemer foregår så korrekt og gnidningsfrit som muligt - eller med andre ord, at interoperabilitet mellem systemer er mulig.

For at interoperabilitet er muligt, er det nødvendigt at standardisere; og i Danmark er der i det offentlige siden 2001 arbejdet målrettet på en sådan standardisering.

Med et fælles sæt af standarder til dataudveksling mellem myndighedernes it-systemer kan den offentlige sektor udvikle it-systemer, hvor informationer er defineret ensartet og kan genbruges på tværs af it-systemerne, så it-systemerne kan anvendes til at skabe sammenhængende services til borgere, virksomheder og andre myndigheder på tværs af forvaltninger og myndigheder.

Hovedprincip for OIOXML

OIOXML er et sprog, der danner grundlaget for at skabe sammenhængende dataudveksling mellem myndighedernes it-systemer, idet OIOXML sikrer, at information udveksles på en ensartet og forståelig måde.

OIOXML er helt konkret en fællesbetegnelse for hele sættet af alle OIO-datastandarder, som samlet udgør det fællesoffentlige udvekslingssprog i XML-format.

Primære virkefelt for OIOXML

Det primære virkefelt for OIOXML er udveksling af information mellem alle offentlige it-systemer udviklet af myndigheder, som er dækket af aftalen om anvendelse af åbne standarder for software i det offentlige.

Obligatoriske, åbne OIOXML standarder

De obligatoriske, åbne standarder er:

- OIO-datastandarder enten adopteret fra internationale bidrag eller udviklet i henhold til den til enhver tid gældende version af det fællesoffentlige regelsæt OIO-NDR (= OIO Navngivnings- og Design Regler).
- XML Schema 1.0 vedligeholdt af W3C (www.w3.org/XML/Schema). OIO-NDR'en er en profil (en nedskåren version) af XML Schema 1.0 anbefalingen, hvor bl.a. (for OIOXML) uhensigtsmæssige konstruktioner er fjernet.
- Extensible Markup Language (XML) 1.0 (Third Edition) vedligeholdt af W3C (http://www.w3.org/TR/2004/REC-xml-20040204)

Anvendelseskrav for OIOXML

At anvende OIOXML vil sige, at al dataudveksling følger specifikationer i eksisterende OIO-datastandarder, herunder at der så vidt muligt (jf. principperne om følg eller forklar) udvikles nye OIO-datastandarder til at tilfredsstille eventuelle udækkede behov. Retningslinierne for anvendelse og udvikling er, som følger:

- for information, som allerede er udtrykt i OIOXML, genbruges eksisterende OIO-datastandarder på den af OIO foreskrevne måde i relevante OIO-retningslinier.
- for information, som endnu ikke er dækket af OIOXML, tilføjes nye OIO-datastandarder efter følgende prioriterede trin:
    1. eksisterer der internationale datastandarder, som dækker det relevante udvekslingsbehov, adopteres disse som OIO-datastandarder, som

>

angivet i relevante OIO-retningslinier (evt. etableres nationale versioner af disse).

2. kun hvor ingen internationale bidrag findes, udvikles nye nationale OIO-datastandarder på den af OIO foreskrevne måde i OIO-NDR'en og andre relevante OIO-retningslinier.

- for nye og bedre versioner af eksisterende OIO-datastandarder, gælder princippet igen, at internationale bidrag til de nye versioner skal prioriteres over nationale.

Standarder til elektronisk sags- og dokumenthåndtering (FESD) >

Den offentlige sektors it-systemer på statsligt, kommunalt og regionalt niveau skal kunne spille sikkert og effektivt sammen. Til dækning af det behov, er der udarbejdet fælles standarder for elektronisk sags- og dokumenthåndtering - de såkaldte FESD-standarder.

Målet med dette standardiseringsarbejde er at fremme digital forvaltning i den offentlige sektor, og midlet er at sikre, at de forskellige elektroniske sags- og dokumenthåndteringssystemer (ESDH) får en fælles kerne, og at det samtidig sikres, at denne kerne videreudvikles ensartet. En fælles kerne skal sikre at:

- at der kan foretages sagsbehandling på tværs af flere organisationer
- at myndigheder, der arbejder med åbne sager, kan lægges sammen
- at der kan flyttes opgaver mellem forskellige myndigheder

Hovedprincip for FESD standarder

ESDH systemer (Elektronisk Sags- og Dokumenthåndtering) i det offentlige skal baseres på en række standarder med henblik på så vidt muligt at sikre interoperabilitet mellem forskellige ESDH systemer samt mellem ESDH systemer og andre systemer (fagsystemer). Den overordnede hensigt er således, at alt så vidt muligt hænger sammen på ESDH-området med henblik på højere kvalitet og bedre effektivitet i sagsbehandlingen.

Primære virkefelt for FESD standardne

Det primære virkefelt for obligatoriske, åbne standarder på ESDH området, er ESDH-systemer, som anskaffes i det offentlige.

Obligatoriske, åbne FESD standarder

De obligatoriske, åbne standarder er:

- FESD Sager og dokumenter
- FESD Adressemodel
- FESD Udvekslingspakke
- FESD Skanningsmodul
- FESD LIS (Ledelsesinformation)

FESD indeholder yderligere syv standarder, der endnu ikke kan gøres obligatoriske, da de endnu ikke er færdigbehandlet. Disse er:

- FESD Udvalgsbehandling
- FESD Brugeradministration
- FESD Arkivstruktur
- FESD Emnesystematik
- FESD Sikker ePostløsning
- FESD Generisk Integrationsmodel
- FESD GIS-Integrationsmodel

Krav om anvendelse af FESD standarderne

At anvende de obligatoriske, åbne standarder for offentlige hjemmesider vil sige, at man

- Implementerer FESD standarderne på den i standarderne foreskrevne måde.

>

Vedligeholdelse af kravet om anvendelse af FESD standarder

OIO-kataloget beskriver løbende hvilke FESD standarder og versioner af disse, der er gældende.

Alle FESD-standarder gennemløber en proces, hvor offentlig høring er et centralt element. Igangsættelse af den enkelte standard sker efter beslutning i den fælles offentlige FESD styregruppe. Det enkelte forslag til standard udarbejdes herefter i fællesskab af de såkaldte FESD-leverandører, hvorefter dette forslag til standard er i offentlig høring i én måned. Efter tilretning på baggrund af den offentlige høring, forelægges forslaget til standard til godkendelse.

Standarder til elektroniske indkøb i det offentlige (OIOUBL) >

Det er målet, at handel mellem den offentlige og private sektor i 2012 skal være fuldt gennemført ved brug af it og åbne standarder. Til indfrielse af det mål, er standarden OIOUBL udviklet.

Udviklingen er sket med følgende tre forretningsmæssige krav for øje:

- Små og store virksomheder og offentlige myndigheder skal med færrest mulige teknologiske, administrative og økonomiske barrierer kunne håndtere de basale elektroniske handelsdokumenter i standarden.
- Handelsdokumenterne skal udvælges med henblik på at være netop det nødvendige og tilstrækkelige sæt af meddelelser, som understøtter den basale indkøbsproces i den offentlige og private sektor.
- Den danske standard skal basere sig på åbne internationale standarder, således at handel over grænser er mulig.

Hovedprincip for elektroniske indkøb

E-handelsdokumenter i den offentlige sektor bør baseres på en række standarder, med henblik på at sikre en nem udveksling af dokumenter mellem den offentlige og den private sektor. Derved sikres, at alle leverandører til den offentlige sektor på forhånd ved hvilket format, de skal understøtte og kan nøjes med at understøtte et frem for mange forskellige formater i deres it-systemer. De offentlige myndigheder får til gengæld mere ensartede og strukturerede data, som giver mulighed for yderligere effektivisering af arbejdsgange og bedre indkøbsstatistikker.

Primære virkefelt for OIOUBL

Det primære virkefelt for obligatoriske, åbne standarder for elektroniske indkøb, er alle offentlige økonomi- og indkøbssystemer anskaffet af myndigheder, som er dækket af aftalen om anvendelse af åbne standarder for software i det offentlige.

Obligatoriske, åbne OIOUBL standarder

De obligatoriske, åbne standarder er:

- OIOUBL version 2.01 vedligeholdt af IT- og Telestyrelsen.
- UN/SPSC version 7.0401 vedligeholdt af GS1.

OIOUBL er en dansk tilpasning af den internationale standard UBL 2.0 fra standardiseringsorganet OASIS (Organization for the Advancement of Structured Information Standards) til danske forretningskrav. OIOUBL indeholder standarder for alle væsentlige forretningsdokumenter til understøttelse af handelsprocessen fra katalog til faktura. De dokumenter, der er medtaget i OIOUBL, og som udgør en delmængde af UBL 2.0 dokumenterne, er udvalgt i samråd med Sektorstandardiseringsudvalget for e-handel.

UN/SPSC UNSPSC (United Nations Standard Product and Services Code) er et internationalt klassifikationssystem for varer og tjenester. Det bruges til at skabe overblik over virksomheders forbrug og foretage systematiske søgninger i forbindelse med elektronisk varekataloger. Det er UNDP (United Nations Development Programme), som ejer rettighederne til UN/SPSC klassifikationssystemet. Systemet administreres i det daglige af GS1 US. GS1 Denmark administrerer i samarbejde med IT- og Telestyrelsen den danske oversættelse af UN/SPSC 7.0401

>

Anvendelseskrav for OIOUBL

At anvende de obligatoriske, åbne standarder for elektronisk ordreafgivelse vil sige, at man

- efterlever OIOUBL specifikationerne som beskrevet i IT- og Telestyrelsens vejledninger på http://www.oioubl.info/classes/da/index.html (dansk version) og http://www.oioubl.info/classes/en/index.html (engelsk version)
- efterlever UN/SPSC klassifikationerne som beskrevet af GS1 på http://www.ean.dk/unspscdk3/index.htm

Standarder for digital signatur

>

Med den digitale signatur har den offentlige sektor etableret en solid infrastruktur for sikker elektronisk identifikation og kommunikation, der er fundamentet for den digitale forvaltning og for etablering af en ny generation af serviceorienterede offentlige og private internettjenester.

Den offentlige sektor vil via etablering af e-services og brug af digital signatur kunne forbedre servicen til borgere og virksomheder samtidig med, at effektiviteten i administrationen øges.

OCES standarden for digital signatur er udviklet for at nedbryde en række barrierer identificeret, efter et tidligere forsøg i 2001 på at stimulere markedet til øget anvendelse af digitale signaturer baseret på kvalificerede signaturer jf. EU-direktiv 1999/93 om en fællesskabsramme for elektroniske signaturer..

Det viste sig i 2001, at markedets forretningsmodeller ikke fungerede, især fordi man som borger selv skulle betale for sin digitale signatur. Hertil kom manglende standardisering og ringe interoperabilitet på tværs af markedets tilbud.

Hovedprincip for OCES digital signatur

Offentlige myndigheder skal som udgangspunkt basere sin digitale forvaltning på anvendelsen af OCES digital signatur i forbindelse med implementering af sikker e-mail og selvbetjeningsløsninger der kræver identifikation og autenticitet. OCES standarden er fastlagt i OCES certifikatpolitikker, som administreres og reguleres af IT- og Telestyrelsen. Certfikatpolitikkerne, der har været sendt i offentlig høring, definerer således et standardiseret og offentligt kontrolleret sikkerhedsniveau for udstedelse og anvendelse af den digitale signatur.

Primære virkefelt for OCES digital signatur

Det primære anvendelsesområde for OCES digital signatur, er kommunikationen mellem borgere, virksomheder og den offentlige sektor, særligt i forbindelse med implementering af sikre e-mail- og selvbetjeningsløsninger.

Obligatoriske, åbne OCES standarder

De obligatoriske, åbne standarder er:

- OCES-personcertifikatpolitik.
- OCES-medarbejdercertifikatpolitik.
- OCES-virksomhedscertifikatpolitik.
- OCES-funktionscertifikatpolitik.

OCES-certifikatpolitikkerne er baseret på nedennævnte internationale standarder, men er tilrettet i forhold til lovmæssige og forvaltningsmæssige krav i den danske digitale forvaltning.

CEN Workshop Agreement 14167-2:2002: ”Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – part 2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)”

ETSI TS 102 042 v 1.2.1. (2005-05): ”Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”

>

ETSI SR 002 176 v 1.1.1. (2003-03): ”Algorithms and Parameters for Secure Electronic Signatures”

FIPS PUB 140-1: “Security Requirements for Cryptographic Modules”

ISO/IEC 15408 (del 1 til 3): ”Information technology - Security techniques - Evaluation criteria for IT security"

ISO/IEC 9794-8/ITU-T Recommendation X.509: ”Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks”

Anvendelseskrav for OCES digital signatur

At anvende den obligatoriske, OCES standard for digital signatur vil sige, at man

- Implementerer sikre e-mailløsninger med anvendelse af OCES digital signatur.
- Implementerer selvbetjeningsløsninger, der anvender OCES digital signatur, hvor der er behov for autentifikation eller elektronisk signatur.

Vedligeholdelse af kravet om anvendelse af OCES digital signatur

De angivne OCES-certifikatpolitikker vedligeholdes og opdateres løbende af IT- og Telestyrelsen. Ved større revisioner gennemføres offentlig høring i forbindelse med revisionen.

De til enhver tid gældende versioner af certifikatpolitikkerne er tilgængelige på www.signatursekretariatet.dk

Standarder for offentlige netsteder og tilgængelighed >

Principperne for forvaltningens digitale kommunikation med borgere og virksomheder bør følge almindelig forvaltningsskik om åbenhed, faglighed og saglighed i behandlingen af borgerne.

Dette betyder, at forvaltningens digitale kommunikation med borgere og virksomheder for så vidt muligt skal sikre:

- at alle har lige adgang til at benytte digitale services, og
- at alle har lige adgang til at kommunikere digitalt med forvaltningen.

God forvaltningsskik foreskriver, at regler og anbefalinger så vidt muligt skrives og udvikles teknologineutralt og produktneutralt. Tilsvarende bør den offentlige forvaltning basere sin borger- og virksomhedsvendte digitale forvaltning på kendte og tilgængelige datastandarder, der understøttes af en lang række producenter.

Forvaltningen bør i sit teknologivalg søge at begrænse de tekniske udgifter og administrative byrder, som pålægges borgeren eller virksomheden, der ønsker at kommunikere digitalt med forvaltningen. Der skal ligeledes tænkes et særligt hensyn til tilgængelighed for blandt andre syns-, bevæge- og hørehæmmede borgere og medarbejdere.

Derfor skal alle nye offentlige netsteder baseres på internationalt anerkendte åbne standarder.

Hovedprincip for offentlige netsteder

Offentlige hjemmesider baseres på en række standarder med henblik på at sikre, at de er tilgængelige for alle borgere og virksomheder. Ved at benytte de obligatoriske standarder sikres, at hjemmesiderne er så fremtidssikrede som muligt og kan bruges bredt på tværs af platforme og værktøjer. Ikke mindst sikres borgere med permament eller midlertidig funktionsnedsættelse digital adgang til det offentlige.

Primære virkefelt for standarder for offentlige netsteder

Det primære virkefelt for obligatoriske, åbne standarder for netsteder er alle offentlige hjemmesider udarbejdet af myndigheder, som er dækket af aftalen om anvendelse af åbne standarder for software i det offentlige.

Obligatoriske, åbne standarder for offentlige netsteder

De obligatoriske, åbne standarder er:

- HTML eller XHTML vedligeholdt af W3C (World Wide Web Consortium).
- CSS vedligeholdt af W3C.
- WCAG (Web Content Accessibility Guidelines), seneste version, level AA, vedligeholdt af WAI (Web Accessibility Initiative) under W3C.

Anvendelseskrav standarder for offentlige netsteder

At anvende de obligatoriske, åbne standarder for offentlige hjemmesider vil sige, at man

- Anvender den version af HTML, XHTML og CSS, man foretrækker på den af W3C foreskrevne måde.
- At man efterlever WCAG level AA. En praktisk vejledning til efterlevelse kan findes på www.itst.dk.

Standarder for it-sikkerhed (DS484)

>

For at styrke den generelle it-sikkerhed i staten skal alle statens institutioner følge en fælles statslig it-sikkerhedsstandard, med mindre særlige økonomiske eller juridiske forhold taler imod.

Hovedprincip for informationssikkerhed

Statslige myndigheder skal basere styringen af deres informationssikkerhed på DS484, "Standard for informationssikkerhed".

DS484 er en national standard, der tager sit udgangspunkt i den vejledende internationale standard ISO17799:2005 (ISO27002). DS484 indeholder en række basale og skærpede krav. Alle basale krav skal som minimum være etableret for at man kan påberåbe sig efterlevelse af standarden.

DS484 er en metodestandard. Valg af konkrete udførelsesmåder og løsningsmodeller i forhold til standardens krav overlades i vidt omfang til den enkelte institution. Udgangspunktet for informationssikkerheden er risikobaseret tilgang hvor risici og løsningsmodeller afvejes. Det afgørende er, at ledelsen eksplicit tager stilling til en risikovurdering, som beskriver hvilken relevans og betydning de enkelte krav har for institutionen og institutionens samarbejdspartnere.

Primære virkefelt for DS484

Det primære virkefelt for DS484 er hele organisationens informationsbehandling. Standardens organisatoriske "fodspor" er således ikke begrænset til it-afdelingen. Endvidere kan standarden, direkte eller indirekte, stille visse generiske krav til organisationens tekniske installationer og fysiske indretning.

Kun gældende for staten

Beslutningen er obligatorisk for alle institutioner, der er underlagt "Bekendtgørelse om statens regnskabsvæsen mv." - i det følgende benævnt regnskabsbekendtgørelsen.

- Ifølge regnskabsbekendtgørelsens § 2 omfatter dette alle: "statsinstitutioner, dvs. departementer, underliggende institutioner, særlige fonde mv., samt selvejende institutioner, der er optaget på bevillingslovene på lige fod med de egentlige statsinstitutioner". Disse statslige institutioner er forpligtede til at følge den fælles standard for it-sikkerhedsprocesser.
- Selvejende institutioner, foreninger, fonde mv., hvis regnskaber omfattes af statsregnskabslovens § 2, stk. 2 er ligeledes forpligtet til at følge den fælles standard for it-sikkerhedsprocesser i staten, såfremt de respektive ressortministerier har taget en sådan beslutning.

De statslige aktieselskaber og selvstændige forvaltningssubjekter er som udgangspunkt ikke underlagt det statslige budget- og bevillingssystem og er dermed ikke omfattet af regeringsbeslutningen.

Bemærk, at dette krav dækker flere statslige institutioner, end de i hovedaftalen beskrevne.

Bemærk endvidere, at dette krav ikke dækker kommuner og regioner.

Obligatoriske, åbne standarder for informationssikkerhed

De obligatoriske, åbne standarder er:

- DS484:2005, vedligeholdt af Dansk Standard

>

Anvendelseskrav for DS484

At anvende DS484 vil sige, at man

- Har forankret styringen af informationssikkerheden i topledelsen, bl.a. ved etablering af et formaliseret styringssystem – et såkaldt Informations Security Management System (ISMS), f.eks. som beskrevet i ISO 27001.
- Har placeret et entydigt ansvar for informationssikkerhed hos ledelsen og, med udgangspunkt i en risikovurdering, formuleret og udmeldt retningslinier som mindst dækker de basale krav i DS484.
- Har omsat retningslinierne til konkrete løsninger og/eller forretningsgange, som efterleves og vedligeholdes løbende.
- Løbende følger op på udvalgte indikatorer for organisationens sikkerhedstilstand og herudfra genererer et passende niveau af ledelsesinformation.

Standarder for dokumentudveksling (ODF/OOXML)

>

Udveksling af tekstbehandlingsdokumenter mellem offentlige myndigheder foregår i dag oftest med formater, som er ejet af de respektive leverandører.

Idet det i dag er muligt at basere udvekslingen af tekstbehandlingsdokumenter på åbne formater, bør det offentlige skifte til at udveksle tekstbehandlingsdokumenter ved brug af disse åbne formater. Dette giver mulighed for større konkurrence og mindre binding til enkeltleverandører.

Hovedprincip for dokumentstandarder

Offentlige myndigheder skal kunne modtage tekstbehandlingsdokumenter fra borgere, virksomheder og andre myndigheder i de åbne tekstbehandlingsdokumentformater OOXML og ODF.

It-løsninger, der indkøbes efter 1. januar 2008, skal understøtte mindst en af de åbne tekstbehandlingsdokumentstandarder ODF og OOXML, og kunne modtage tekstbehandlingsdokumenter i begge formater, evt. ved brug af tilføjelsesprogrammer (convertere, plug-ins).

Om ODF og /eller OOXML skal være obligatoriske efter 1. juli 2009 afgøres efter en vurdering af en uafhængig tredjepart.

Primære virkefelt for dokumentstandarder

De primære virkefelter er

- udveksling af redigerbare tekstbehandlingsdokumenter mellem offentlige myndigheder og
- modtagelse af redigerbare tekstbehandlingsdokumenter fra borgere, virksomheder og myndigheder.

Obligatoriske, åbne dokumentstandarder

De obligatoriske, åbne standarder er:

- ODF (Open Document Format) vedligeholdt af standardiseringsorganisationen OASIS.
- OOXML (Office Open-XML) vedligeholdt af ECMA.

Anvendelseskrav for dokumentstandarder

- Fra den 1. januar 2008 skal alle myndigheder sikre, at de kan modtage dokumenter i de to formater.
- Ved anskaffelse af nye systemer efter 1. januar 2008 skal offentlige myndigheder sikre sig, at disse kan understøtte et eller begge de beskrevne formater.

Vedligeholdelse af kravet om dokumentstandarder

Om ODF og /eller OOXML skal være obligatoriske, åbne standarder efter 1. juli 2009 afgøres efter en vurdering af en uafhængig tredjepart.

Som led i vurderingen indgår blandt andet:

- Softwareleverandørernes evne til at sikre interoperabilitet mellem de to standarder i deres produkter i forhold til det offentliges udvekslingsbehov (funktionalitetsloft).

>

- De reelle muligheder for og de praktiske erfaringer med at implementere standarderne uafhængigt af leverandør og platform.
- En konkret vurdering fra Konkurrencestyrelsen om effekten af anvendelse af obligatoriske åbne standarder for dokumentudveksling på konkurrencesituationen.

OIO-kataloget

>

OIO-kataloget er den fællesoffentlige ressource til brug ved planlægning og udvikling af offentlige it-projekter. OIO-kataloget indeholder beskrivelser og vurderinger af udvalgte standarder, teknologier og protokoller, som ønskes anvendt og understøttet i forbindelse med udbygningen af digital forvaltning i Danmark.

OIO-kataloget bør være kendt af offentlige myndigheder, som udvikler it-strategier, -planer og -projekter, og af disses leverandører og rådgivere. Intentionen er at bidrage til at sikre bedre sammenhæng og teknisk konsistens ved anvendelse af etablerede teknologier i hele den danske offentlige sektor.

International forankring af OIO-kataloget

Standardisering giver ofte ikke mening i en snæver dansk sammenhæng. Dette skyldes dels, at der sker datasamspil over grænserne, dels at standardiseringen i praksis i mange tilfælde skal udføres af leverandører, som retter sig imod det internationale marked. Derfor skal standardiseringen i Danmark gennemføres i forlængelse af det internationale arbejde på området.

I EU-regi kaldes OIO-kataloget en national interoperabilitetsramme for digital forvaltning (e-Government Interoperability Framework). En national interoperabilitetsramme tilbyder et sæt politikker, tekniske standarder og retningslinjer (anbefalet praksis), som skitserer forvaltningens politik med hensyn til, hvordan interoperabilitet skal opnås. Den nationale interoperabilitetsramme er rettet mod alle myndigheder, som har behov for at interoperere med andre myndigheder og med deres øvrige omverden, herunder EU og andre medlemslande.

Inden for rammerne af det Europæiske samarbejde om digital forvaltning er udarbejdet en særlig pan-europæisk interoperabilitetsramme (European Interoperability Framework, EIF), der skal ses som et supplement til de nationale rammer. OIO-kataloget er udarbejdet i overensstemmelse med EIF. Der er fortsat behov for kontinuerligt at foretage justeringer for at sikre overensstemmelse med EIF.

Justeringer af OIO-kataloget

OIO-kataloget har under flere navne eksisteret siden 2003. Udviklingen gennem de seneste fire år og kravene i forbindelse med obligatoriske åbne standarder bevirker naturligt nok, at det er nødvendigt at revidere strukturen og indholdet af kataloget med henblik på, at dette bliver tilrettet de nye krav.

Indførelsen af obligatoriske åbne standarder i det offentlige tager sit udgangspunkt i det eksisterende fællesoffentlige standardiseringsarbejde. Kontinuitet er nøgleordet, og udgangspunktet for indførelsen af obligatoriske åbne standarder ligger i forlængelse af det standardiseringsarbejde, der allerede har foregået i flere år i det fællesoffentlige samarbejde forankret i IT- og Telestyrelsen.

Målet I forbindelse med indførelsen af obligatoriske åbne standarder tilvejebringes af en bedre anvendelse og værdi af det fremadrettede arbejde med eksisterende standarder. Denne tilpasning viser sig klarest på tre punkter.

>

1 *Rådgivning.* IT- og Telestyrelsen har hidtil rådgivet om, hvilke standarder der blev anset som de bedste. Nu bliver visse standarder obligatoriske at anvende, med mindre væsentlige argumenter taler imod. Introduktion af *følg eller forklar*-begrebet fordrer, at offentlige myndigheder skal begrunde, hvis de ikke lever op til OIO-katalogets krav om obligatoriske standarder.

2 *Dokumentation.* Der er et klart behov for, at beslutningerne om hvilke kriterier, der ligger til grund for godkendelsen af standarder, i højere grad bliver dokumenteret.

3 *Vedligeholdelse.* Med et sæt af obligatoriske åbne standarder, skal der løbende være fokus på udviklingen vedr. standardiseringsområdet, den tekniske/markedsmæssige udvikling og den forretningsmæssige udvikling

OIO-katalogets struktur

OIO-kataloget inddeler standarder i tre overordnede kategorier. Tekniske standarder, datastandarder og metodestandarder.

Karakteristik af de tre typer standarder

Tekniske standarder
Det er karakteristisk for tekniske standarder, at de har fokus på it-systemers *tekniske* virkemåde. Hovedformålet med fastsættelse af tekniske standarder er at sikre tekniske løsninger, der understøtter den samlede arkitektur og dermed fremmer hvidbogens fem hovedprincipper, som beskrevet i afsnit 3.3 ”Principper for it-arkitektur”.

Datastandarder
Det er karakteristisk for datastandarder, at de har fokus på de *data*, der registreres, anvendes og udveksles i forskellige systemer og organisationer. Formålet med datastandarder er at skabe grundlag for mere integrerede løsninger og for genbrug af data.

Metodestandarder
Det er karakteristisk for metodestandarder, at de har fokus på *måden*, hvorpå der arbejdes i digitaliseringsprojekter og i forbindelse med udvikling og drift af it-løsninger. Det er også et særtræk, at der er relativt få metodestandarder. Formålet med metodestandarder er at skabe løsninger af kvalitet, sammenhæng, interoperabilitet og tillid.

Nye obligatoriske, åbne standarder

>

Obligatoriske, åbne standarder er udvalgte og navngivne standarder, som er vurderet hensigtsmæssige for anvendelse i den offentlige sektor.

Fastsættelse af obligatoriske, åbne standarder sker efter indstilling fra videnskabsministeren og kræver beslutning i regeringen samt aftale med de de kommunale og regionale parter.

Til grund for beslutningen skal foreligge en faglig og økonomisk vurdering af det enkelte sæt af standarder.

Den faglige vurdering skal blandt andet belyse, om der er tale om en åben standard, hvilken forretningsmæssig relevans standarden har for den offentlige sektor og om markedsmæssige forhold gør standarden klar til anvendelse. Den faglige vurdering skal gøres til genstand for en offentlig høring.

Hvis den faglige vurdering viser, at der er tale om en potentiel obligatorisk, åben standard, skal der efterfølgende laves en økonomisk konsekvensvurdering, der blandt andet skal afdække, om det er uden meromkostninger for det offentlige, at gøre standarden til en obligatorisk, åben standard.

>

<

Vejledning om anvendelse af obligatoriske, åbne standarder for software i det offentlige

Fra den 1. januar 2008 bliver en række åbne standarder obligatoriske at anvende for alle offentlige myndigheder. Det betyder, at alle nye offentlige it-løsninger skal kunne anvende disse obligatoriske, åbne standarder.

Den 1. januar 2008 vil en række åbne standarder blive obligatoriske at anvende for offentlige myndigheder ved fremtidige indkøb af software og it-løsninger.

For offentlige myndigheder betyder det, at man skal sikre sig, at fremtidige it-løsninger er baseret på eller understøtter, disse obligatoriske, åbne standarder, hvis standarderne er relevante for it-løsningen.

For alle de obligatoriske, åbne standarder gælder, at den enkelte myndighed ved eventuelle merudgifter eller for den pågældende myndighed it-sikkerhedsmæssige hensyn kan undlade at anvende de obligatoriske standarder.