



FESD Datafølgеседdel

Høring

Dette udkast til forslag til FESD-standard er i offentlig høring i perioden fra 12. juli 2007 til 22 august 2007.

IT- og Telestyrelsen København 12. juli 2007

FESD-standardisering

FESD Datafølgеседdel. Protokol Version 0.8

Kolofon:

FESD-standardisering. FESD Datafølgeseddel. Protokol. Version 0.8

Denne standard kan frit anvendes af alle. Citeres der fra standarden i andre publikationer til offentligheden, skal der angives korrekt kildehenvisning.

Forslag til FESD-standarder udarbejdes af IT- og Telestyrelsen, IT-Arkitektur kontoret, FESD-standardiseringsgruppen i samarbejde med de tre FESD-leverandører Software Innovation A/S, Accenture I/S og CSC Danmark A/S.

Kontaktperson i FESD-standardisering:

Projektleder Palle Aagaard, Mailadresse paa@itst.dk

Telefon 33 37 92 67 (direkte)

Accenture A/S

Arne Jacobsens Allé 15
2300 København S
Telefon: 72 28 80 00
Web-adresse: <http://www.accenture-fesd.dk/>

CSC Danmark A/S

Retortvej 8
1780 København V
Telefon: 36 14 40 00
Web-adresse: <http://www.fesd-alliancen.dk/>

Software Innovation A/S

Nærum Hovedgade 10
DK-2850 Nærum
Telefon: 45 58 88 88
Web-adresse: <http://www.softwareinnovation.dk/>

Ministeriet for Videnskab, Teknologi og Udvikling IT- og Telestyrelsen

IT-Arkitektur kontoret

National IT and Telecom Agency
Ministry of Science, Technology and Innovation
Holsteinsgade 63
DK-2100 København Ø
Telf. +45 35 45 00 00
Fax. +45 35 45 00 10
<http://www.itst.dk>
itst@itst.dk

Indholdsfortegnelse

1. FORORD	5
1.1 Teknisk forord.....	5
2. DEL A – FESD DATAFØLGESEDDER	7
1.2 Indledning.....	7
1.3 Sammenhæng med DOKFORM og FESD Packet standarderne	7
1.3.1 Formål.....	7
1.3.2 Afgrænsning.....	7
3. DEL B – FORRETNINGSARKITEKTUR	8
1.4 Datafølgeseddlens anvendelse	8
1.5 Ansvar	8
1.6 Protokoller	8
1.7 Web-Service til modtagelse af datafølgeseddel	9
1.8 Transaktionshåndtering	10
1.8.1 Gentagen oversendelse / opdatering	11
1.8.2 Unik identifikator for sags- og dokumentobjekter	11
1.8.3 Datafølgeseddlens struktur.....	12
1.8.4 Myndigheds- eller sektorspecifikke udvidelser af skemaet	13
1.8.5 Anvendelse af myndigheds- eller sektorspecifikke udvidelser af skemaet.....	14
Anvendelse af myndigheds- eller sektorspecifikke udvidelser af skemaet.....	14
1.8.6 Elektronisk signering og kryptering af datafølgeseddel	15
DEL C – BESKRIVELSE AF SKEMA	16
1.1 Beskrivelse af klasser.....	16
1.1.1 Elementet følgeseddel meta	16
1.1.2 Elementet Sag meta	16
1.1.3 Beskrivelse af elementet SagsPart meta	18
1.1.4 Elementet JournalPost.....	19
1.1.5 Beskrivelse af elementet JournalpostPart meta.....	21
1.1.6 Beskrivelse af elementet Dokument meta.....	24
1.1.7 Beskrivelse af elementet DokumentObjekt	26
1.8.7 Elementet Følgeseddel Signatur	26
4. BILAG A	27
1.2 Anvendte typer i FESD-modellerne	27
1.2.1 integer	27
1.2.2 boolean.....	27
1.2.3 Identifikationstyper	27
1.2.4 char.....	28

1.2.5	date, dateTime og time.....	28
1.2.6	string	29
1.2.7	float	29

1. Forord

Den offentlige sektors IT-systemer på statsligt, kommunalt og regionalt niveau skal kunne spille sikkert og effektivt sammen. Derfor arbejdes der målrettet på at få gennemført fælles standarder for elektronisk sags- og dokumenthåndtering - den såkaldte FESD-standard. Målet med standardiseringsarbejdet 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 kernefunktionalitet, og at det samtidig sikres, at denne kerne videreudvikles ensartet. En fælles kernefunktionalitet skal sikre:

- 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

I forlængelse af FESD-projektkonkurrencen, som havde sin afslutning primo 2004, og hvor der blev fundet tre FESD-leverandører, blev det i forbindelse med kontraktforhandlingerne besluttet at starte en standardiseringsproces – den såkaldte FESD-standardisering.

For at sikre interoperabiliteten, både mellem ESDH-systemer og til andre systemer, men også så tredjepart kan udvikle moduler til systemet, blev det anset for afgørende, at der udvikles en fælles offentlig datamodel samt andre standarder på ESDH-området.

Koordinering af FESD-standardiseringen er efterfølgende lagt i IT- og Telestyrelsen (ITST). Den konkrete udarbejdelse af forslag/udkast til standarder foregår i et samarbejde mellem de tre FESD-leverandører og en FESD-standardiseringsgruppe i ITST.

Arbejdet med forslag/udkast til standarder tager udgangspunkt i Noark 4's datamodel og databeskrivelser samt leverandørernes løsninger. Standarderne kan afvige fra Noark 4 på de områder, hvor det er nødvendigt for at understøtte dansk forvaltningspraksis, eller hvor parterne i FESD-standardiseringen kan opnå enighed om en afvigelse.

Udkast/forslag sendes herefter i offentlig høring i ca. 1 måned. FESD-standardiseringsgruppen tilretter og færdiggør på baggrund af høringen de endelige "Forslag til standarder".

Standardforslagene forelægges herefter OIO-Datastandardiseringskomiteen til godkendelse.

Efter den samlede godkendelse bliver standarderne således offentliggjort og indgår i IT- og Telestyrelsens "OIO-Katalog", som indeholder en oversigt over godkendte og anbefalede standarder til digital forvaltning i det offentlige.

I standarden kan forekomme brug af særligt ordvalg. Følgende termer anvendes konsekvent i den følgende betydning:

- **"skal"/"obligatorisk"**: betyder, at den nævnte metode/element/mulighed/etc. skal benyttes eller skal forefindes – dvs. må ikke udelades.
- **"må ikke"**: betyder, at den nævnte metode/element/mulighed/etc. ikke må forefindes eller må ikke benyttes.
- **"bør"/"anbefalet"**: betyder, at det i høj grad anbefales, at den nævnte metode/element/mulighed/etc. benyttes eller forefindes. Der skal være tungtvejende grunde til at udelade.
- **"kan"/"optionel"**: betyder, at den nævnte metode/element/mulighed/etc. er en valgmulighed og derfor valgfri at medtage.

1.1 Teknisk forord

Grundlaget for FESD-datamodellen er blevet udarbejdet på en periode på mere end 2 år, hvor der er udarbejdet standarder for de forskellige delområder. Arbejdsmetoder, terminologi og anvendelse af datatyper har ændret sig i denne periode – FESD-standardiseringsgruppen har f.eks. indført en konsekvent brug af UML-notation i de senere standarder. Konsolideringen af datamodellen har derfor forudsat, at der blev defineret en

fælles modelleringsmetode og et sæt af primitive datatyper, der var kompatibelt med alle del-datamodellerne. De primitive datatyper, som modellen er opbygget af, fremgår af bilag A.

2. DEL A – FESD Datafølgeseeddel

1.2 Indledning

Standarden FESD Datafølgeseeddel – i det følgende betegnet som datafølgeseedlen - angiver struktur og indhold for en datafølgeseeddel der kan benyttes til oversendelse af sags- og dokumentinformation mellem myndigheder, uden forudgående aftale.

Datafølgeseedlen kan sidestilles med en almindelig brevforsendelse mellem myndigheder, med den forskel at datafølgeseedlen giver den modtagende part alle relevante oplysninger om sags, dokument og part i elektronisk form, som grundlag for registrering

Datafølgeseedlen er en videreudvikling af FESD Packet, som gav mulighed for at sende dokumenter mellem myndigheder, baseret på DOKFORM standarden i forhold til beskrivelse af dokumenterne. Datafølgeseedlen giver også mulighed for at medsende information om sag og part, og udvider dermed anvendelsesmulighederne i forhold til FESD Packet.

Datafølgeseedlen tager indholdsmæssigt udgangspunkt i FESD Datamodel, og sags- og parts- og dokumentinformation er således umiddelbart sammenligneligt med FESD Datamodel.

1.3 Sammenhæng med DOKFORM og FESD Packet standarderne

FESD Packet standarden specificerer hvorledes dokumenter sendes mellem myndigheder, baseret på DOKFORM eller udvekslingskernen som den også kaldes. FESD Packet er begrænset til at sende dokumenter via e-post, og havde dermed en række begrænsninger i forhold til såvel det indholdsmæssige, som metoder til at sende.

Datafølgeseedlen giver mulighed for at benytte andre protokoller end SMTP (e-mail), og giver desuden mulighed for at sende information om sag og part i tilknytning til dokumenterne. Forsendelser med datafølgeseedlen, beriger således forsendelsen i et større omfang end FESD Packet gav mulighed for.

Datafølgeseedlen afløser FESD Packet, og udgør det der i FESD Packet standarden betegnes som FASE 2. Der vil ikke ske yderligere revisioner af FESD Packet, ligesom der sandsynligvis heller ikke vil blive udarbejdet flere revisioner af DOKFORM (Udvekslingskernen).

1.3.1 Formål

Formålet med standarden FESD Datafølgeseeddel, er at give et grundlag for fremsendelse af sager og dokumenter fra en myndighed til en anden, og dermed understøtte behovet for sagsbehandling på tværs af myndighederne i den offentlige forvaltning.

1.3.2 Afgrænsning

Standarden for FESD Datafølgeseeddel har sit udgangspunkt i FESD Packet standarden, og i FESD kontraktens krav om understøttelse af eFølgeseddel såvel ved afsendelse som modtagelse af dokumenter i FESD systemet. Standarden baserer sig ikke på eller har sit udgangspunkt i den norske NOARK-4 standard, som det er tilfældet for andre FESD standarder.

Standarden stiller ikke eksplicite krav til implementering af forretningslogik, til understøttelse af udveksling baseret på datafølgeseedlen, men FESD kontraktens krav om at FESD systemet skal kunne danne og afsende en e-følgeseddel baseret på udvekslingskernen, samt modtage og anvende samme som registreringsgrundlag, vil være gældende i forhold til datafølgeseedlen.

Anvendelse af de forskellige protokoller, beskrevet i afsnit 1.6 vil variere fra leverandør til leverandør, og der kan kun forventes en understøttelse, svarende til den eksisterende, baseret på udvekslingskernen.

3. Del B – Forretningsarkitektur

1.4 Datafølgesejlens anvendelse

Datafølgesejlen giver mulighed for at en myndighed kan sende sager og dokumenter til en anden myndighed, i elektronisk form. Forsendelsen indeholder, udover de elektroniske dokumenter, de metadata den afsendende myndighed har registreret i sit FESD ESDH system, og giver således den modtagende myndighed et grundlag for registrering af tilsvarende metadata i sit FESD ESDH system. Dermed opnår den modtagende myndighed dels en større præcision i sin registrering, dels en effektivitetsgevinst idet en tidligere registrering genbruges.

Det er vigtigt at bemærke, at der i forvaltningsmæssig forstand er tale om forskellige instanser af hhv. sager og dokumenter hos den afsendende og modtagende myndighed.

Nedenstående figur illustrerer den forretningsgang, datafølgesejlen er tænkt anvendt:

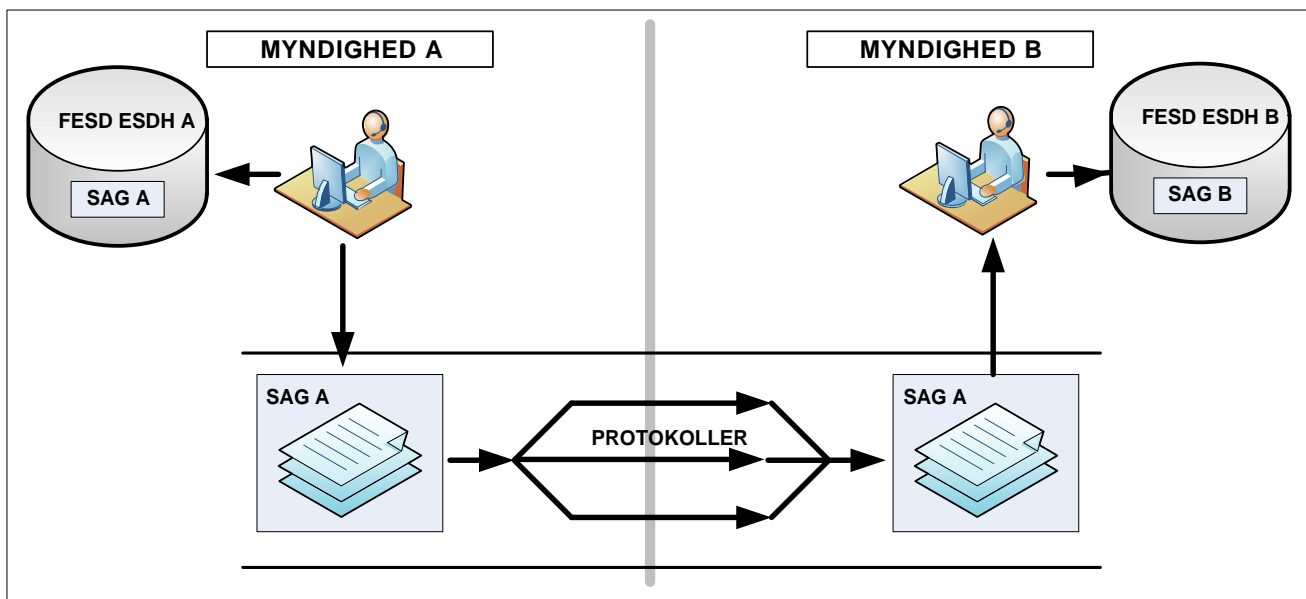


Fig. 1 – Forretningsgang for oversendelse af datafølgesejle

I forbindelse med et sagsforløb, som involverer to myndigheder, udfører myndighed A sin sagsbehandling til et givent punkt, og sagen skal herefter behandles i myndighed B. Myndighed A danner en datafølgesejle indeholdende information om sagen, sagens dokumenter og de elektroniske dokumenter, og sender denne via en af de mulige protokoller til myndighed B. Myndighed B anvender det fremsendte som grundlag for registrering af sagen/dokumenterne i sit FESD ESDH system.

1.5 Ansvar

Det er den afsendende part som har ansvaret for oversendelsen, herunder modtagelsen, til den modtagende part. Det vil sige at det er den afsendende part der skal sikre at den oversendte information er modtaget og vil blive behandlet som ønsket.

Standarden giver ikke mulighed for f.eks. anmodning om kvittering for modtagelse eller behandling. Den afsendende part må foretage en implementering af datafølgesejlen, som i nødvendigt omfang sikrer afsendelse/modtagelse i henhold til de krav der gælder for kommunikationen mellem de to parter. Dette kan ske gennem valg af protokol og evt. gennem særskilt aftale mellem afsender og modtager.

1.6 Protokoller

Til forskel fra FESD Packet, som alene forholder sig til benyttelse af SMTP (e-post), kan man sende datafølgesejlen ved hjælp af flere protokoller:

SMTP	Oversendelse via e-post. Denne protokol er i dag understøttet af FESD Packet standarden, og er den protokol der typisk anvendes. Protokollen er asynkron. Det vil sige at man ikke umiddelbart får en kvittering for modtagelse, og ikke har 100% sikkerhed for modtagelse.
FTP	Oversendelse via FTP protokollen kan anvendes i forbindelse med oversendelse af større data mængder. Herudover har protokollen den fordel at man får en teknisk kvittering på at oversendelse er gennemført.
FILE	Ved oversendelse af større datamængder, eller oversendelse til en myndighed som ikke har åbnet for direkte kommunikation, kan protokollen FILE anvendes. I praksis vil oversendelsen skulle ske via et fysisk medie (CD, DVD, USB-memory stick, ell. lign.). Mediet transporteres fysisk fra afsender til modtager. Man kan opnå kvittering for modtagelse, gennem traditionelle forsendelsesmetoder (post / bud / fragt).
HTTP	I de tilfælde hvor man har hyppig oversendelse af data fra en myndighed til en anden, f.eks. i de tilfælde hvor to myndigheder i fællesskab forvalter et sagsområde, kan det være hensigtsmæssigt at pgl. myndigheder udvikler web-services som benyttes til oversendelsen.

Ved valg af protokol, er der flere ting som bør overvejes:

- 1) Tekniske muligheder for kommunikation
- 2) Behovet for kvittering for oversendelse/modtagelse
- 3) Datamængder

Selve datafølgesejden er identisk, uanset valgt protokol, men omfanget i forbindelse med implementering, og den opnåede sikkerhed i forbindelse med overførsel vil variere meget.

1.7 Web-Service til modtagelse af datafølgesejdel

Som en del af standarden defineres en webservice ved navn **receiveFESDDeliveryNote**, som skal kunne modtage en datafølgesejdel og behandle denne med henblik på registrering i et ESDH system.

Da en datafølgesejdel per definition kun kan fungere som et registreringsgrundlag kan den interne funktionalitet i servicen ikke beskrives, og det vil være frit for den enkelte leverandør at afgøre graden af manuel sagsbehandling i forbindelse med en oversendelse. Servicen har således til formål at sikre, at det er muligt at sende datafølgesejden problemfrit via http-protokollen, og kravet er således blot at servicen tager en datafølgesejdel som argument.

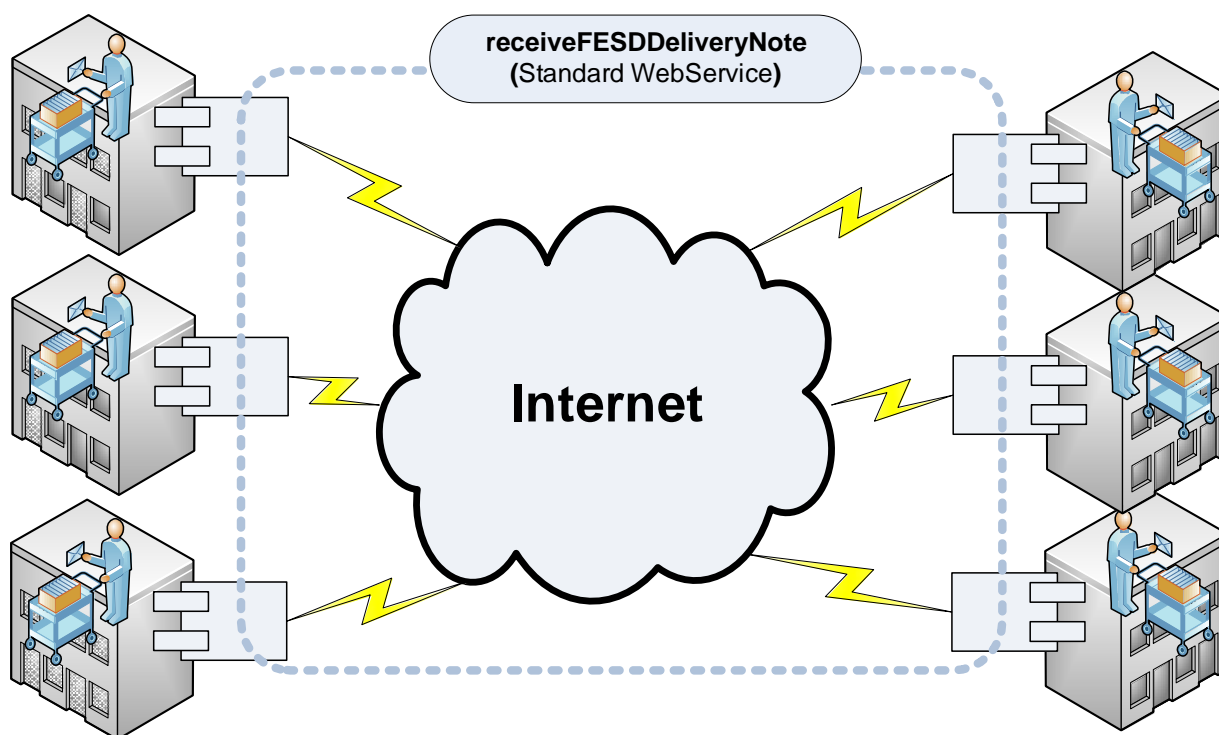


Fig. 2 – Netværk af myndigheder der udstiller en dedikeret Web-Service til modtagelse af datafølgerseddel

Webservicen skal implementeres via en realisering af OWSA model T (OIO Web Service Arkitektur model Transportbaseret sikkerhed) referencemodellen.

OWSA model T er baseret på punkt-tilpunkt kommunikation over SSL 3.0. Dermed sikres fortroligheden i forbindelse med overførsel af data, og datafølgerseddelen behøver ikke særskilt kryptering.

OWSA model T er endvidere relevant da denne standard realiserer både MOCES(medarbejdercertifikat) og VOCES(virksomhedscertifikat). Det er således muligt som myndighed at eksponere en webservice til modtagelse af datafølgersedler og samtidigt sætte konkrete regler for hvilke myndigheder eller sagsbehandlere der kan tilgå denne service, og sikre en pålidelig identifikation af samme.

Dette personcertifikat skal ikke forveksles med den signering som foregår på selve datafølgerseddelen. Signering af datafølgerseddel har til formål at sikre uafviselighed af data på tværs af protokoller, hvorimod certifikatet som oversendes med webservicekaldet har til formål at bevise brugsretten af pågældende service.

I takt med implementering af standarden i den offentlige sektor, vil de implementerede Web-Services udgøre et alternativt forsendelsesnet. Standarden indeholder ikke administrative retningslinier i forhold til lokalisering og anvendelse af en modtagelsesservice hos en specifik myndighed. Det forventes her at den eksisterende infrastruktur omkring OIO/ISB benyttes. Myndighedernes web-services vil dermed være udstillet i det centrale UDDI.

1.8 Transaktionshåndtering

Datafølgersedlen er udviklet med henblik på effektiv oversendelse af sags- og dokumentinformation, herunder dokumentobjekter.

Standarden indeholder ikke mulighed for f.eks. at afsender kan anmode om modtagelseskvittering af modtageren.

Krav om pålidelighed, kvittering, mv. skal adresseres i forbindelse med valg af protokol, og evt. gennem bilaterale aftaler mellem afsender og modtager.

Høj pålidelighed i forbindelse med oversendelse opnås gennem anvendelse af http protokollen. Det vil sige gennem en dedikert webservice, som modtageren udstiller. Her vil man umiddelbart få en kvittering for transaktionen og dermed for teknisk modtagelse af den oversendte pakke.

Tilsvarende vil man ved anvendelse af protokollen FTP kunne opnå en teknisk transmissionskvittering.

I forhold til anvendelse af FILE og SMTP protokollerne, som begge er asynkrone protokoller, er der ikke umiddelbart mulighed for at opnå kvittering for modtagelse, og bør således ikke benyttes hvis det er et krav i forbindelse med oversendelsen.

1.8.1 Gentagen oversendelse / opdatering

I forbindelse med hyppig kommunikation mellem to myndigheder, kan man forestille sig et behov for at den ene myndighed sender en sag med sags dokumenter, og på et senere tidspunkt ønsker at sende samme sag, med opdaterede oplysninger samt yderligere dokumenter.

Opdatering er ikke medtaget som en del af standarden, og de to oversendelser er – i forhold til standarden – selvstændige, uafhængige forsendelser. Evt. semantik omkring opdatering af sagsinformation, tilføjede dokumenter siden sidste forsendelse, mv. skal aftales bilateralt mellem afsender og modtager.

Til støtte for fastlægge af semantik omkring gentagen oversendelse, indeholder standarden krav om entydig identifikation af sags- og dokumentobjekter – se afsnit 1.8.2 vedrørende unikke identifikatorer.

1.8.2 Unik identifikator for sags- og dokumentobjekter

Oversendelse af sager mellem myndigheder kan ske på et vilkårligt tidspunkt i sagsforløbet, og kan i nogle tilfælde ske flere gange:

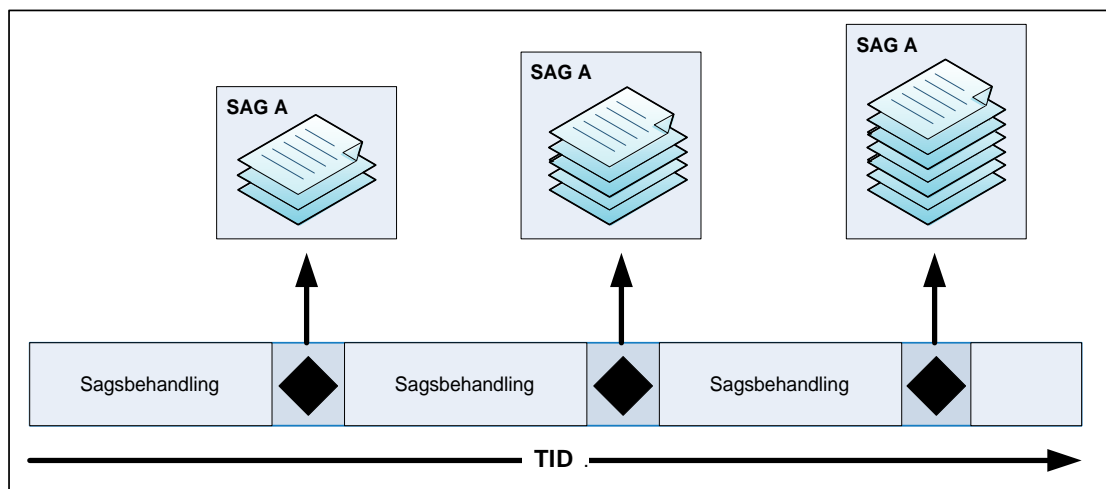


Fig. 3 – Sagens udvikling over tid, med flere oversendelser.

Ovenstående figur, illustrerer et sagsforløb, hvor den samme sag sendes fra en myndighed til en anden, flere gange indenfor det specifikke sagsforløb. Sagen vil udvikle sig over tid, det vil sige at der vil være flere dokumenter i sagen, sags metadata vil muligvis ændre sig, osv.

Standarden giver ikke mulighed for at DELETE en sag mellem to myndigheder – det vil sige at der ikke er elementer eller metoder som specifikt skal bidrage til at sikre synkronisering af sags- og dokumentinformation mellem to myndigheder.

Imidlertid er der et krav om at den afsendende part opmærker afsendte sager og dokumenter med en unik identifikator, som skal benyttes ved en evt. senere oversendelse af samme sag/dokument eller ved oversendelse til en tredje myndighed.

Den unikke identifikator, anbefales konstrueret efter følgende princip:

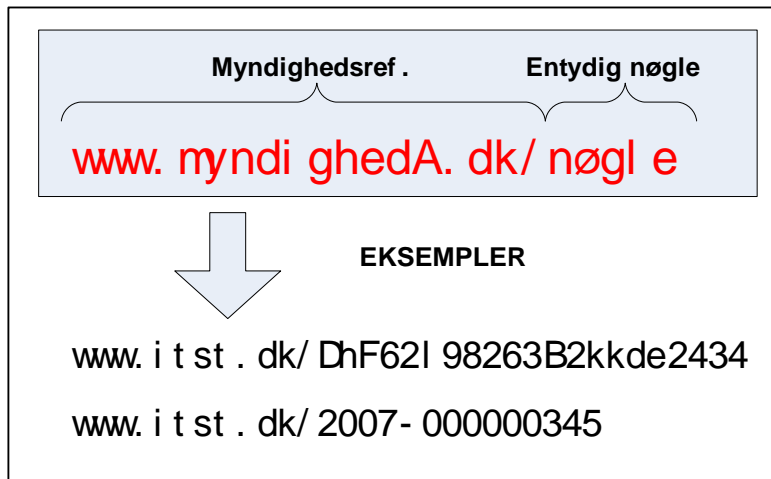


Fig. 4 – Konstruktion af unik identifikator

Afsendende myndighed har ansvaret for at danne en unik reference, der over tid er persistent. Referencens formål er primært at kunne identificere et sags- eller dokumentobjekt der oversendes mere end en gang, men kan også benyttes som reference i andre former for dialog mellem myndigheder.

1.8.3 Datafølgesedlens struktur

Datafølgesedlen indeholder en sag og et eller flere dokumenter, samt parter på både sags- og dokumentniveau. Dokumenter skal i denne sammenhæng forstås som journalposter der kan indeholde flere dokumenter - både metadata om dokumenter og selve dokumentobjektet.

Strukturen følger strukturen i FESD Datamodel, med SAG-JOURNALPOST-DOKUMENT-DOKUMENTVERSION. Der er dog foretaget en sammenlægning af klasserne DOKUMENT og DOKUMENTVERSION, idet datafølgesedlen ikke understøtter oversendelse af flere versioner af samme dokument. Det antages, at en myndighed ved oversendelse af et dokument, sender seneste officielle/godkendte version.

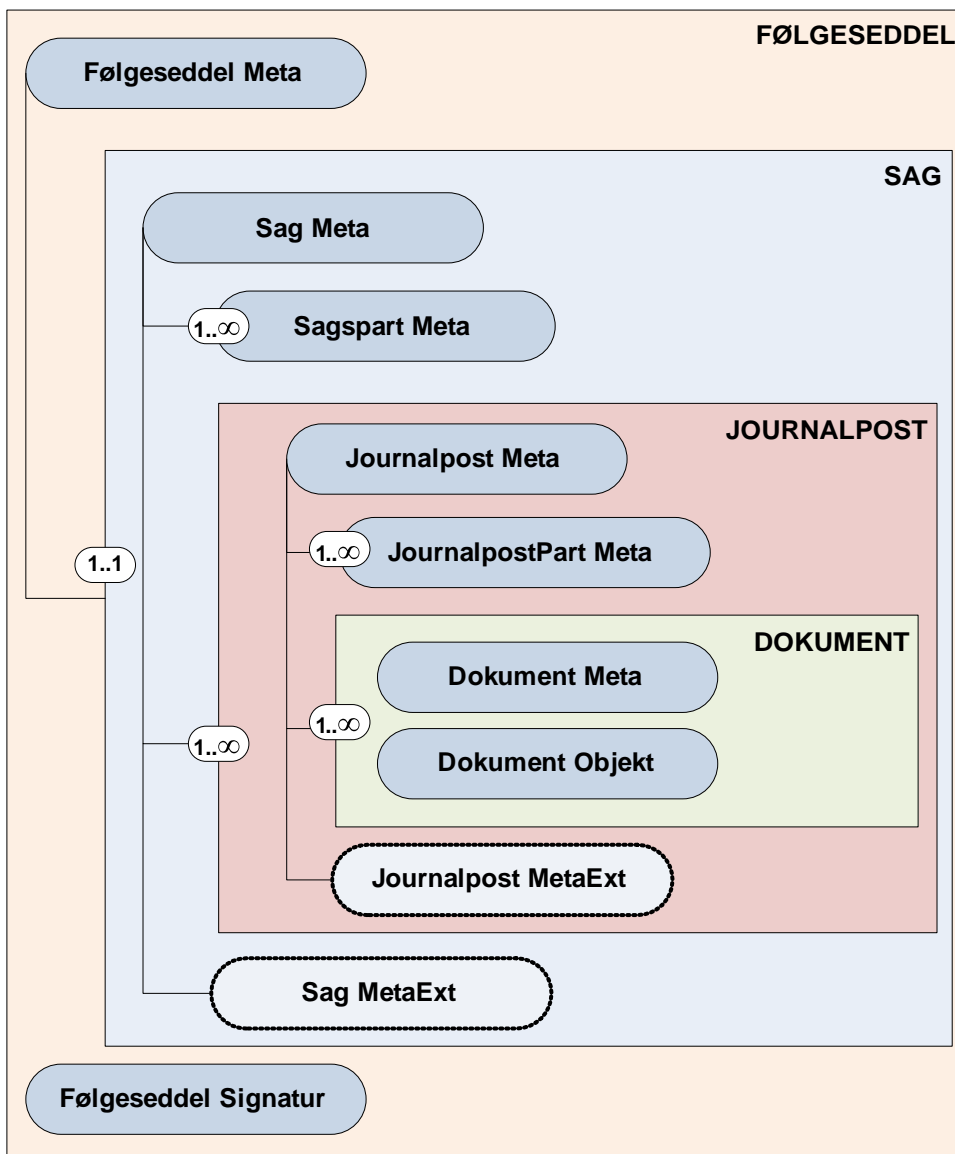


Fig. 5 – FESD datafølgeseddel opbygning

Dokumentobjekter (filer) inkluderes i datafølgesedlen, som kodede objekter, ved benyttelse af base64 encoding. Datafølgesedlen vil således kun bestå af ét filobjekt – et XML-dokument, indeholdende såvel metadata som dokumentobjekter (filer). I forhold til dokumentformater, indeholder standarden ingen begrænsninger. I og med der benyttes Base64 encoding, neutraliseres det oprindelige format.

Det betyder, at den enkelte myndighed må vurdere hvilke formater det er hensigtsmæssigt at anvende ved oversendelse til en anden myndighed. Man bør anvende formater der er generelt accepteret som produktions- og/eller arkiveringsformater, for at sikre at modtageren er i stand til at læse/benytte de oversendte dokumenter.

Elementet DOKUMENT giver mulighed for en simpel angivelse af hvilket format et givent dokument oversendes i. Angivelsen foretages ved at specificere ekstension samt en verbal beskrivelse af formatet.

1.8.4 Myndigheds- eller sektorspecifikke udvidelser af skemaet

Datafølgesedlen indeholder generelle metadata for sager, dokumenter og parter. Normalt vil disse være dækkende i forhold til at beskrive de sager og dokumenter der oversendes, men der kan være behov for sektorspecifikke eller myndighedsspecifikke metadata, som vil kunne berige de oversendte sager/dokumenter og dermed potentielt berige en given sagsproces.

Datafølgersedlen indeholder derfor en mulighed for udvidelse, som kan benyttes. Udvidelsesmuligheden kan benyttes indenfor de nedenfor beskrevne restriktioner.

1.8.5 Anvendelse af myndigheds- eller sektorspecifikke udvidelser af skemaet

Datafølgersedlen indeholder generelle metadata for sager, dokumenter og parter. Normalt vil disse være dækkende i forhold til at beskrive de sager og dokumenter der oversendes, men der kan være behov for sektorspecifikke eller myndighedsspecifikke metadata, som vil kunne berige de oversendte sager/dokumenter og dermed potentielt berige en given sagsproces.

Datafølgersedlen indeholder derfor en mulighed for udvidelse, som kan benyttes. Udvidelsesmuligheden kan benyttes med de nedenfor beskrevne restriktioner.

Anvendelse af myndigheds- eller sektorspecifikke udvidelser af skemaet

Overordnet kan den påtænkte udvidelsesmulighed illustreres på følgende måde:

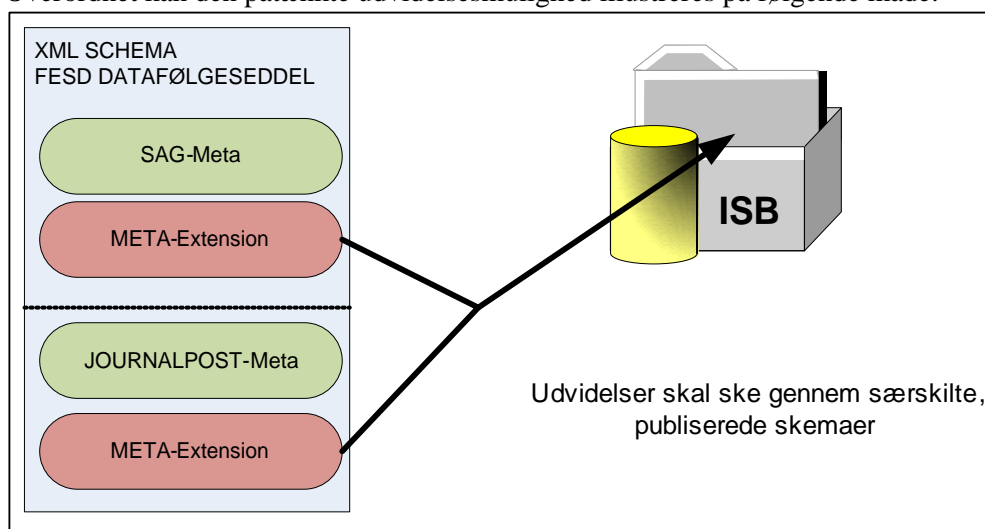


Fig. 6 – Udvidelseselementer i datafølgersedlen

De to udvidelsesformer dækker:

- 1) Beskrivende metadata om sagen
Yderligere, beskrivende attributter om sagen
- 2) Beskrivende metadata om dokumentet
Yderligere, beskrivende attributter om dokumentet

Tilføjelse af de to typer af udvidelser, realiseres gennem et såkaldt ANY element, der som bekendt kan benyttes uden restriktioner i XML skemaet. En fri modellering af ANY elementet, vil svække standarden, og elementet vil således kun kunne benyttes indenfor standarden, såfremt en række betingelser er overholdt:

- 1) Udvidelser skal realiseres gennem særskilte skemaer, som er publiceret på ISB'en
- 2) Skemaerne skal følge NDR reglerne i forhold til udformning, mv.
- 3) Skemaerne skal formålsbeskrives, og må ikke dække generelle forhold som rettelig skal adresseres i standarden og ikke som en udvidelse.
- 4) Der skal være reference til ansvarshavende for udvidelsen

Kravet om publicering af udvidelserne betyder at modtageren vil være i stand til at validere de udvidelser der er foretaget. Det vil også betyde, at standardiseringsenheden vil kunne opsamle og vurdere de forskellige udvi-

delser der foretages, med henblik på at revidere standarden, og evt. tilføje yderligere, generelle metadata til standarden.

1.8.6 Elektronisk signering og kryptering af datafølgeseeddel

Et vigtigt element i FESD Datafølgeseeddel, er muligheden for at signere følgesedlen, standardiseret og dermed uafhængigt af specifikke produkter, og uafhængig af hvilken protokol man benytter i forbindelse med oversendelse.

I datafølgeseedlen anvendes XML-Signature (xmldsig) til at påføre digitale signaturer. Den fulde beskrivelse af xmldsig ligger udenfor dette dokumentets formål og kan findes på <http://www.w3.org/TR/xmldsig-core/>.

Datafølgeseedlen tillader et ubegrænset antal personer at signere følgesedlen, og det vil således være muligt at implementere en procedure hvor en sagsbehandler forbereder og danner følgesedlen, signerer denne digitalt og fremsender til nærmeste leder for godkendelse, inden afsendelse.

Tilsvarende vil en modtager af datafølgeseedlen kunne signere denne, og dermed tilføje endnu en signatur til følgesedlen, hvorefter den kan videresendes indeholdende alle digitale underskrifter.

Signatur kan påføres datafølgeseedlen som helhed. Standarden giver ikke mulighed for at signere enkelte dele af følgesedlen.

Signeringen foretages, som tidligere nævnt, uafhængig af den protokol der påtænkes anvendt. En signeret datafølgeseeddel kan således oversendes via e-post, på en CD, via ftp, mv., i signeret form.

Anderledes forholder det sig med kryptering. Standarden ser kryptering som værende knyttet til transport. Det vil sige til de protokoller som er nævnt i afsnit 1.6 Protokoller.

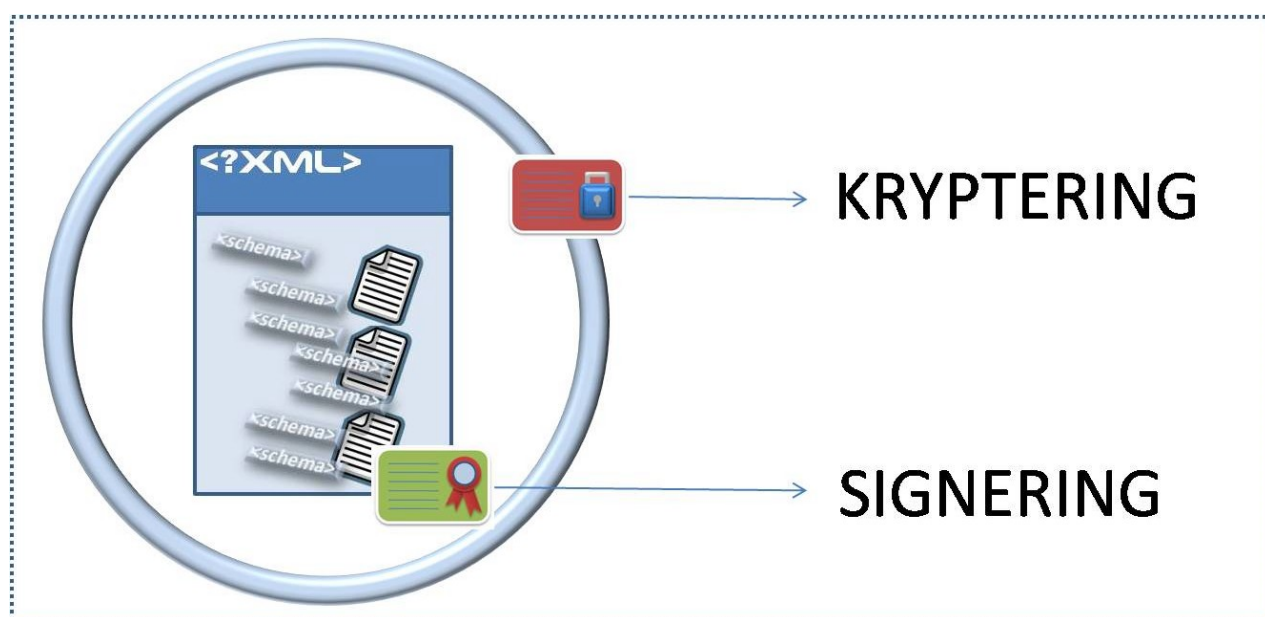


Fig. 7 – Adskillelse af signering og kryptering af datafølgeseedlen

Ovenstående figur, illustrerer adskillelsen af signering og kryptering. Signeringen foretages på datafølgeseedlen, og først når datafølgeseedlen afsendes, krypteres den forsendelse som datafølgeseedlen udgør.

Det vil dermed være muligt at anvende krypteringsfaciliteterne i det e-post programmel man anvender, man kan vælge at benytte liniekryptering ved oversendelse via http (https), mv.

Del C – Beskrivelse af skema

1.1 Beskrivelse af klasser

1.1.1 Elementet følgeseddel meta

Indeholder overordnet information om datafølgesedlen

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse
dfsAfsenderNavn	dnSenderName	char(50)	[1]	Afsender myndighedsnavn
dfsAfsenderCVR	dnSenderCVRReference	int(8)	[1]	Afsenders CVRnummer.
dfsAfsenderKontaktpersonNavn	dnSenderContact-Name	char(50)	[1]	Personnavn på vedkommende der er ansvarlig for afsendelse af følgesedlen, og som dermed bør kontaktes i forhold til den specifikke oversendelse.
dfsAfsendelsesDatoTid	dfsSenderDateTime	DateTime		CCYYMMDD, Jf. ISO 8601.

1.1.2 Elementet Sag meta

Indeholder information om sagen med hovedvægt på de traditionelle journaloplysninger.

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse
sagIdentifikatir	caseFileIdentifier	anyURI	[1]	Unik nummerering af samtlige sager for at sikre teknisk entydighed. Anvendes som teknisk reference for sagen, hvilket muliggør skabelse af referentiel integritet. UUID (Universal Unique Identifier) anvendes (jf. ISO/IEC 9834-8:2005 fra International Telecommunication Union). Anføres på formen: urn:uuid:<uuid-identifiser>
sagPapir	caseFilePaperStorageIndicator	char(1)	[0..1]	Angiver om sagen arkiveres på papirform eller elektronisk. Værdi der angiver, om sagen er på papir eller elektronisk.
sagDato	caseFileCreationDate	Date	[1]	Oprettelsesdato for sagen. Bør tildeles automatisk. Anvendes som bl.a. afgrænsningsparameter ved søgninger. Sagsoprettelsesdato CCYYMMDD, Jf. ISO 8601.

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse
sagTitel	caseFileTitleText	char(255)	[1]	Feltet indeholder sagens titel, der er ingen krav om entydighed, blot at titlen afspejler sagens indhold. Feltet bidrager sammen med journalnummer/emneord og andre sagsinformationer til at sagsbehandleren/journalføreren kan vurdere sagens indhold og dermed relevans for den opgave, vedkommende skal løse. Felt indeholder sagens titel i klar tekst.
sagTitelUofficiel	caseFileTitleUnofficialIndicator	Indicator	[1]	Værdi der markerer, om sagstitlen er officiel. Markerer om sagstitlen indeholder fortrolig information, eller af anden grund ikke er officiel.
sagTitelAlternativ	caseFileTitleAlternativeText	char(255)	[0..1]	Hvis sagstitlen er uofficiel kan dette felt indeholde en alternativ officiel sagstitel, til postlister etc. Feltet indeholder en alternativ titel i klar tekst.
sagsStatusBetegnelse	caseFileStatusName	ShortText	[1]	Sagsstatus betegnelse i klar tekst. Fri tekst.
sagsTypeBetegnelse	caseFileTypeName	ShortText	[1]	Sagstypebetegnelsen i klar tekst. Anvendes til at beskrive en række sagstyper, der kan indgå i sagsbehandlingen.
sagAnsvarligSagsbehandler	caseFileManagerReference	char(50)	[1]	Feltet udfyldes med navn på ansvarlig sagsbehandler. Hentes fra Bruger.brugerNavn
sagUndtagetOffentlighed	caseFileRestrictedFromPublicText	ShortText	[0..1]	Henvielse til den lovgivning under hvilken denne sag er undtaget offentlighedsloven. Udfyldes med henvisning til den lovgivning, hvis hjemmel anvendes for at undtage sagen fra almindelig offentlighed. Der vil ofte være tale om persondataskyttelseslovgivningen eller lign. Fri tekst.
sagSenesteJournalPost	caseFileLatestRecordDate	Date	[0..1]	Udfyldes med dato for seneste registrerede journalpost. Angiver hvornår der senest har været tilføjet journalposter i sagen. Der er ikke sammenhæng til rækkefølgen af dokumenter. Bør være automatisk genereret dato af seneste tilføjelse af journalpost.
sagSletningsfrist	caseFileRetentionTimeYear	integer(2)	[0..1]	Antal år sagen skal bevares. Anvendes typisk i forbindelse med Kassationsbestemmelser fra Statens Arkiver og/eller sletningsfrister jf. Registerforeskriften fra Datatilsynet. Antal år CC.
kassationsKodeBetegnelse	disposalName	ShortText	[1]	KassationsKoden i klar tekst. Beskriver kassationskoden.
sagKassationDato	caseFileDisposalDate	Date	[0..1]	Angiver hvornår der skal foretages kassation eller anden arkivmæssig behandling af sagen. Kassation skal jf. Persondataskyttelsesloven foregå på et givent tidspunkt. Der skal eventuelt ske aflevering til Statens Arkiver inden. Denne dato angiver hvornår der skal foretages kassation. Kassationsdato

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse
				CCYYMMDD, Jf. ISO 8601.
sagNr	caseFileNumberIdentifier	char(40)	[1]	Frit sagsnr. Eventuelt sammenstillinger af andre felter. Indeholder ofte journalnummeret, der traditionelt er sammenstillinger af forskellige andre felter fra Sag og Registrering eksempelvis sagsår, sagGruppe og sagLoebenummer. Frit sagsnummer. Fri tekst.
sagAfsluttetDato	caseFileClosedDate	Date	[0..1]	Udfyldes med den dato sagen opfattes som afsluttet CCYYMMDD, Jf. ISO 8601
sagNormtid	caseFileEstimatedTime	Integer(3)	[0..1]	Evt. fastsat normtid i dage for behandling af sagen
sagNettosagsbehandlingstid	CaseFileActualWork	Integer(3)	[0..1]	Skønnet nettosagsbehandlingstid i dage. Dvs. antal kalenderdage brugt til egentlig behandling af sagen og dermed undtaget de dage hvor sagen behandles udenfor institutionen (er i høring, behandles af anden institution, afventer svar fra part etc.)
emneIdentifikator	termIdentifier	char(34)	[1]	Dette er den entydige identifikator for emnet indenfor systematikken. Identifikatoren er en streng, hvor tilladte karakterer er alle alfanumeriske tegn plus tegnet punktum ('.').
emneKvalificeretEmneID	termUniqueTermIdentifier	anyURI	[1]	Dette er en generelt entydig identifikator for emnet. Identifikatoren er en URI dannet ved sammensætning af den URI-baserede identifikator for emnesystematikken + URI-fragmentsymbolet '#' + emneID. Denne ID skal gøre det muligt for eksterne parter og systemer entydigt at genkende og identificere klassificering foretaget med emnesystematikken. I tilfælde, hvor der foretages lovlige udvidelser af en emnesystematik med eksternt forfatter, udvides identifikatoren for emnesystematikken med en organisationsreference.
EmneDeskriptorTekst	termDescriptorText	Text	[1]	Kortfattet, præcis titel for emnet.

1.1.3 Beskrivelse af elementet SagsPart meta

Indeholder information om sagens parter. Part skal her forstås bredt, som personer, organisationer, genstande, mv. Elementet er primært opbygget af elementer fra FESD adressemodel, som ikke beskrives her. Der henvises til beskrivelse af adressemodellen på oio.dk:

<http://www.oio.dk/index.php?o=bd8a9c1811c3c28a6786e1319110ef89>

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse
sagsPartRolle	caseFileReferenceRole	ShortText	[0..1]	Den rolle (part, fuldmægtig advokat eller lign.) kontaktpersonen har i sagen. Fri tekst. Eventuelt hentet fra opslagstabel.
sagsPartUofficielIndikator	caseFileReferenceUnOfficialIndicator	Indicator	[0..1]	Udfyldes hvis oplysninger om sagsparten er undtaget almindelig offentlighed. Hvis sagsparten er en person, må sagspartsoplysningerne ikke umiddelbart offentliggøres. Der kan også findes andre årsager til at sagspartsoplysningerne ikke umiddelbart må offentliggøres. Værdi, hvortil der bør anvendes følgende udfaldsrum: 1 hvis sagsparten ikke umiddelbart kan offentliggøres ellers 0.
sagsPartKommentar	caseFileReferenceComment	Text	[0..1]	Kommentar der beskriver sagspartens forhold til sagen. Fri tekst.

1.1.4 Elementet JournalPost

Indeholder grundoplysningerne om en Journalpost. Anvendes til at registrere grundoplysninger om hoveddokument, eventuelt med underdokumenter og/eller bilag.

Attribut Dan	Attribut Eng	Type	Kardinalitet	Beskrivelse
journalPostID	recordIdentifier	anyURI	[1]	Unik nummerering af samtlige Journalposten for at sikre teknisk entydighed. Anvendes som teknisk reference for Journalposten, hvilket muliggør skabelse af referentiel integritet. UUID (Universal Unique Identifier) anvendes (jf. ISO/IEC 9834-8:2005 fra International Telecommunication Union).). Anføres på formen: urn:uuid:<uuid-identificer>
journalPostDokumentNummer	recordSequenceNumber	char (4)	[1]	Dokumentnummeret indenfor sagen. Anvendes til at definere dokumentets rækkefølge i sagen. I Noark 4 tildeles nummeret automatisk og kan kun ændres ved en flytning eller omregistrering af sagen. Entydigt maskingenereret løbenummer knyttet til dokument i sagen.
journalPostRegistreringsDato	recordRegistrationDate	date	[1]	Registreringsdato for journalposten. Anvendes til at registrere det tidspunkt, hvor journalposten er registreret i systemet. Retningslinierne for udfyldelsen af dette felt bør hænge sammen med processen for modtagelse af dokumenter. Registreringsdato CCYYMMDD, Jf. ISO 8601.
dokumentTypeBetegnelse	documentTypeName	ShortText	[1]	Dokumenttypen i klar tekst.
journalPostDokumentDato	recordDocumentDate	Date	[1]	Dokumentdato for dokumentet. Anvendes til at registrere den dato, der er påstemplet eller på anden måde registreret på dokumentet. Dokumentdato CCYYMMDD, Jf. ISO 8601.
journalPostUdateret	recordDocumentDateUnknownIndicator	Indicator	[1]	Værdi der dokumenterer, om dokumentet er udateret. Et dokument betragtes som udateret, hvis det ikke er muligt at lokalisere en dato af brevhederen

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse
				eller specifikt markeret som afsendelsesdato.
journalPostIndholdsBeskrivelse	recordDescriptionText	Text	[1]	Tekst der beskriver indholdet af journalposten. Anvendes til at beskrive indholdet af journalposten, der kan være tale om et hoveddokument med underdokumenter, eller bilag, eller enkeltstående dokumenter. Fri tekst. Om journalposten.
journalPostIndholdsBeskrivelseUofficiel	recordDescriptionUnofficialIndicator	char (1)	[0..1]	Udfyldes hvis oplysninger om Journalpostens indholdsbeskrivelse er undtaget almindelig offentlighed. Hvis beskrivelsen af journalpostens indhold indeholder personoplysninger, eller anden fortrolig information markeres det i dette felt.
journalPostIndholdsBeskrivelsAlternativ	recordAlternativeDescriptionText	Text	[0..1]	Kan indeholde en alternativ beskrivelse. Hvis indholdsbeskrivelse af journalpost er uofficiel, kan dette felt indeholde en alternativ officiel journalpost beskrivelse til postlister etc.
journalPostAfskrivningsDato	recordDeprecationDate	date	[0..1]	Registrerer dato for hvornår dokumentet er færdigbehandlet. I den offentlige forvaltning skal det sikres, at alle henvendelser besvares, og at de besvares indenfor en given tidsramme. Feltet anvendes som basisinformation for denne type af opgaver. Færdigbehandletdato CCYYMMDD, Jf. ISO 8601.
journalPostEkspederetDato	recordResponseDate	date	[0..1]	Registrerer dato for hvornår dokumentet er ekspederet. Knytter sig til sagsbehandlingsdelen af systemet. Ekspeditionsdato CCYYMMDD, Jf. ISO 8601.
journalPostforfaldsDato	recordResponseDeadlineDate	date	[0..1]	Forfaldsdato registrerer, hvornår dokumentet senest skal være ekspederet. Knytter sig til sagsbehandlingsdelen af systemet. Fristdato for ekspedition CCYYMMDD, Jf. ISO 8601.
journalPostUndtagetOffentlighed	recordPublicationIndicator	ShortText	[0..1]	Henvisning til den lovgivning under hvilken denne journalPost er undtaget offentlighedsloven. Udfyldes hvis journalPosten er undtaget fra almindelig offentlighed. Udfyldes med henvisning til den lovgivning, hvis hjemmel anvendes for at undtage journalPosten fra almindelig offentlighed. Der vil ofte være tale om persondatabeskyttelseslovgivningen eller lign. Fri tekst.
journalPostOffentlighedsvurderet	recordPublicationEvaluationDate	Date	[0..1]	Dato for hvornår journalposten er blevet offentlighedsvurderet. Anvendes til at beskrive hvornår Journalposten er blevet offentlighedsvurderet. Kan anvendes i forbindelse med aktindsigtsregler og/eller åbne postlister. Offentlighedsvurderet dato CCYYMMDD, Jf. ISO 8601.
journalPostPapirIndikator	recordPaperStorageIndicator	Indicator	[1]	Skal journalposten arkiveres i papirform eller elektronisk. Angiver om journalposten arkiveres på papirform eller elektronisk.
journalStatusBetegnelse	recordStatusName	ShortText	[1]	Journalstatus i klar tekst. Beskriver Journalstatus.
journalPostAnsvarligSagsbehand-	recordCaseManagerRef-	Char(50)	[0..1]	Udfyldes med information om hvem der er ansvarlig sagsbehandler.

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse
ler	rence			Hentes fra Bruger.brugerNavn
journalPostAnsvarligEnhed	recordRecipientUnitReference	char(50)	[0..1]	Udfyldes med information om ansvarlig organisation/afdeling for journalposten. Enhedsnavnet hentes fra OrgEnhed.enhedsNavn
journalPostSkanDato	recordScanDate	Date	[0..1]	Datoen hentes fra scanDateTime efter evt. skanning. Formatet er CCYYDDMM, jf. ISO 8601
journalPostSkanTid	recordScanTime	Time	[0..1]	Tidspunktet hentes fra scanDateTime efter evt. skanning. Formatet er hh:mm:ss, jf. ISO 8601
journalPostSikkerhedsKlassifikation	recordSecurityClassification	char(50)	[0..1]	Sikkerhedsklassifikationskode. Sikkerhedsklassifikation er beskrevet i FES-Dstandarden for BrugerAdministration.
journalPostKategoriKode	recordCategoryCode	Code	[0..1]	Kategori af Journalposten. Denne kan være indgående, udgående, notat. Udfyldes med I, U, N.

1.1.5 Beskrivelse af elementet JournalpostPart meta

Indeholder information (navn adresse etc.) som beskriver den/de person, virksomhed, myndighed eller organisation, som er part i dokumentet (afsender/modtager).

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse
personCprNr	personCPRNumber	integer(10)	0 -1	Entydig identifikation på en person. Noter at cprNr <u>ikke</u> fungerer som entydig identifikator for klassen, da cprNr ikke kan forventes kendt for alle instanser. Udfyldes såfremt personOrganisationIndikator angiver at der er tale om en person.
personAdresseringsNavn	personAddressName	Name	1	Fornavn, mellemnavn og efternavn, sammenstillet. Elementet er ikke nødvendigvis konstrueret af de selvstændige elementer fornavn, mellemnavn og efternavn, men kan i sin helhed være tolket eller indtastet i forbindelse med indskanningen. Udfyldes såfremt personOrganisationIndikator angiver at der er tale om en person.
personForNavn	personSurName	char(50)	1	Den samlede længde af forNavn må ikke overskride 50 karakterers længde
personMellemNavn	personMiddleName	char(40)	0 -1	Den samlede længde af mellemNavn må ikke overskride 40 karakterers længde
personEfterNavn	personFamilyName	char(40)	1	Feltets indhold kan bestå af flere navne adskilt af en blank position eller af en bindestreg. Feltet kan være blank for børn, hvis disse endnu ikke er navngivet.

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse
organisationCvrNr	organizationCVRNumber	integer(8)	0-1	Afsenderorganisationens CVR nummer. Udfyldes såfremt personOrganisationIndikator angiver at der er tale om en organisation.
organisationOrganisationsNavn	organizationOrganization- Name	char(50)	1	Navnet på organisationen eller virksomheden. Udfyldes såfremt personOrganisationIndikator angiver at der er tale om en organisation.
personOrganisationIndikator	personOrganizationIndicator	indicator	1	Angivelse af om part er en person eller en organisation, og således hvilke oplysninger der skal være tilstede.
adresseKommuneKode	addressMunicipalityCode	char(4)	1	Det af Indenrigsministeriet fastsatte nummer for kommunen. Refererer til klassen 'Kommune'. Herfra kan 'kommuneNavn' hentes.
adresseLandKodeAlfa2	addressCountryCodeAlpha2	Code	1	ISO-betegnelsen for land.
adresseVejKode	addressRoadCode	char(4)	1	Vejkoden består af fire cifre i intervallet 0001-9999. Intervallet 9900-9999 kaldes 'højvejkode' og er afsat til særlig anvendelse. Vejkode angiver koden for den gade/vej, hvor ejendommen/bygningen/enheden er beliggende. Vejkode danner sammen med kommunekode en entydig kode for en vej i Danmark. Refererer til klassen 'Vej'. Herfra kan udledes såvel 'vejNavn' som 'vejAdresseringsNavn'
adresseHusNr	addressHouseNumvber	char(4)	1	Nummerbetegnelse inkl. et evt. stort bogstav, som identificerer en bestemt adgang til en bygning, en grund eller et teknisk anlæg og lign. med udgangspunkt i den navngivne vej som giver adgang hertil. Ved "Husnummer" forstås i Danmark altid husnummer inkl. evt. bogstav. Indgår et bogstav i adressen, er dette en nødvendig del af den fuldstændige og korrekte adresse. Et husnummer består af et tal i intervallet 1-999. Husnummeret kan have tilknyttet et bogstav fra A til Z.
adresseEtag	addressFlorRefernce	char(2)	0 - 1	Etagen, hvor enheden er beliggende. Etagen kan antage følgende værdier: Den etage hvis gulvplan ligger i eller umiddelbart over gadeniveau benævnes ST De følgende etager herover benævnes nedefra og op efter 1, 2, 3, til 99 Kældre (etagerne under gadeniveau) benævnes KL K2 K3 til K9 i retning ovenfra og nedefra Etagen angives ikke, hvis der kun er en enhed i bygningen.
adresseDoerBetegnelse	addressDoorReference	char(4)	0 - 1	Identifikation som beskriver beliggenheden af en bestemt indgangsdør på en etage (trappeafsats) i den pågældende opgang.

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse
				<p>Betegnelserne "tv", "mf" og "th" bruges når der er indtil tre døre på trappe-afsatsen. Hvis der er flere døre anvendes tallene 1, 2, 3, 4 osv. Andre betegnelser på indil 4 tegn kan dog også fastsættes.</p> <p>På etager med fire enheder kan betegnelserne TV, MFTV, MFTH og TH anvendes.</p>
adresseLinie1	addressLine1	char(50)	0-1	c/o reference. Såfremt landeKodeAlfa2 er forskellig fra 'DK', indgår adresselinien uspecificeret i den udenlandske adresse.
adresseLinie2	addressLine2	char(50)	1	Gade, husnummer, etage. Såfremt landeKodeAlfa2 er forskellig fra 'DK', indgår adresselinien uspecificeret i den udenlandske adresse.
adresseLinie3	addressLine3	char(50)	0-1	Såfremt landeKodeAlfa2 er forskellig fra 'DK', indgår adresselinien uspecificeret i den udenlandske adresse. Anvendes ikke hvis landeKodeAlfa2 er 'DK'
adresseLinie4	addressLine4	char(50)	0-1	Såfremt landeKodeAlfa2 er forskellig fra 'DK', indgår adresselinien uspecificeret i den udenlandske adresse. Anvendes ikke hvis landeKodeAlfa2 er 'DK'
adresseLinie5	addressLine5	char(50)	0-1	Såfremt landeKodeAlfa2 er forskellig fra 'DK', indgår adresselinien uspecificeret i den udenlandske adresse. Anvendes ikke hvis landeKodeAlfa2 er 'DK'
adressePostboks	addressPostboxReference	Char(4)	0-1	Nummer eller anden identifikation jf. Post Danmark
adressePostNr	addressZipCode	char(4)	1	Et postnummer består af fire cifre. Refererer til klassen 'PostDistrikt'. Herfra kan 'postDistrikt' hentes (tekstbetegnelse for distriktet)
adresseByNavn	addressCityName	char(34)	1	<p>Det fastsatte bynavn præciserer beliggenheden inden for en kommune eller postdistrikt. Et evt. bynavn er en nødvendig del af den fuldstændige og korrekte adresse. Et bynavn skal fastsættes når der findes ens eller enslydende vejnavne i postdistriktet eller kommunen.</p> <p>byNavn kan bestå af indtil 34 tegn.</p>
adresseLokalitetsNavn	addressSiteName	char(34)	0 - 1	<p>Ikke entydigt navn for lokalitet.</p> <p>lokalitetsNavn (gårdnavn, bygningsnavn e.l.) kan knyttes til en enkelt eller flere adresser i en bygning eller et bygningskompleks</p> <p>lokalitetsNavn består af indtil 34 tegn som indgår i den officielle adressebetegnelse, f.eks. fra CPR</p> <p>Reglerne herom findes i § 17, stk. 3, i Cirkulære om ajourføring af CPRs vej- og boligregister (Cirkulære nr. 130 af 25. november 2002).</p>
ePostAdresse	emailAddressIdentifier	uri:mailto	1	Emailadresse i standard uri-form; <navn>@<domæne>
journalPostfaxNummer	recordPartyFaxNumber	char (20)	-	Faxnummeret på person, virksomhed, myndighed eller organisation der er part i sagen. Faxnummer, eventuelt foranstillet +

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse
journalPostPartTlf	recordPartyPhoneNumber	char (20)	-	Telefonnummer på person, virksomhed, myndighed eller organisation der er part i sagen. Telefonnummer, eventuelt foranstillet +
journalPostPartRolle	recordPartyRole	char (70)	[0..1]	Den rolle (part, fuldmægtig advokat eller lign.) kontaktpersonen har i sagen. Fri tekst. Eventuelt hentet fra opslagstabel.
kontaktNavnAdresseBeskyttelse	contactNameAddressProtection	boolean	1	Markering der viser om personen har navne-/adressebeskyttelse
journalPostPartUofficiel	recordPartyUnofficial	char (1)	[0..1]	Udfyldes hvis oplysninger om journalpostparten er undtaget almindelig offentlighed. Hvis journalpostparten er en person, må journalpostpartsoplysningerne ikke umiddelbart offentliggøres. Der kan også findes andre årsager til at journalpostpartsoplysningerne ikke umiddelbart må offentliggøres. Værdi, hvortil der bør anvendes følgende udfaldsrum: 1 hvis journalpostparten ikke umiddelbart kan offentliggøres ellers 0.

1.1.6 Beskrivelse af elementet Dokument meta

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse	Origin
dokumentID	documentIdentifier	anyURI	[1]	Unik nummerering af samtlige dokumenter for at sikre teknisk entydighed. Anvendes som teknisk reference for dokumenter, hvilket muliggør skabelse af referentiel integritet. UUID (Universal Unique Identifier) anvendes (jf. ISO/IEC 9834-8:2005 fra International Telecommunication Union).). Anføres på formen: urn:uuid:<uuid-identifiser>	Dokument
dokumentKategoriBetegnelse	documentCategoryName	ShortText	[1]	Dokumenttilknytningstypen i klar tekst. Beskriver informationstypen.	DokumentKategori
dokumentTitelTekst	documentTitleText	Text	[1]	Feltet indeholder dokumentets titel, der er ingen krav om entydighed, blot at titlen afspejler dokumentets indhold. Feltet bidrager sammen med andre dokumentinformationer til, at sagsbehandleren/journalføreren kan vurdere dokumentets indhold og dermed relevans for den opgave vedkommende skal løse.	Dokument

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse	Origin
dokumentPaaPapirIndikator	documentPaperStorageIndi- cator	Indicator	[1]	Angiver om sagen arkiveres på papirform eller elek- tronisk.	Dokument
dokumentPapirPlaceringTekst	documentPaperStorageLo- cationText	Text	[0..1]	Fri tekst der angiver papirets fysiske placering. Feltet anvendes til at beskrive, hvor papirdokumenter i form af tykke rapporter, publikationer, der ikke indskannes i deres fulde omfang, fysisk placeres.	Dokument
dokumentStatusBetegnelse	documentStatusName	ShortText	[1]	Dokumentstatus i klar tekst. Beskriver dokumentsta- tus.	DokumentSta- tus
dokumentUdarbejdetAf	documentCreatorReference	Char(50)	[0..n]	Udfyldes med information om hvem der har udarbej- det dokumentet. Hentes fra Bruger.brugerNavn	
dokumentUndtagetOffentlighed- Tekst	documentNonDisclosureText	char(16)	[0..1]	Henvisning til den lovgivning under hvilken dette dokument er undtaget offentlighedsloven. Udfyldes med henvisning til den lovgivning, hvis hjemmel an- vendes for at undtage dokumentet fra almindelig offentlighed. Der vil ofte være tale om persondata- beskyttelseslovgivningen eller lign. Fri tekst.	
dokumentVersionLoebenummer	documentVersionNumber	integer(5)	[1]	Indeholder dokumentets versionnummer indenfor dokumentet. Tildeles ofte automatisk. Entydigt ma- skingenereret løbenummer.	DokumentVer- sion
variantTypeBetegnelse	variantTypeName	ShortText	[1]	Varianten i klar tekst. Beskriver varianten.	VariantType
lagringsFormatFilType	storageFormatDefaultFileTy- pe	LongCode	[0..1]	Angiver standardformat filtyper eksempelvis DOC for Word. Tekst.	
lagringsFormatFilType	storageFormatDefaultFileTy- pe	LongCode	[0..1]	Angiver standardformat filtyper eksempelvis DOC for Word. Tekst.	
dokumentTilknytningsBetegnelse	documentLinkTypeName	ShortText	[1]	dokumentTilknytningsBetegnelse i klar tekst. Beskri- ver informationstypen.	

1.1.7 Beskrivelse af elementet DokumentObjekt

Attribut Dan	Attribut Eng	Type	Kardinali- tet	Beskrivelse	Origin
kodetDokumentObjekt	encodedDocumentObject	Base64binary	[1]	Indeholder dokumentobjekt(fil) i binær, kodet form, med anvendelse af Base64 kodningsstandarden.	

1.8.7 Elementet Følgeseddel Signatur

I FESDpacket anvendes XML Signature (xmldsig) til at signere datafølgседlen. Den fulde beskrivelse af xmldsig ligger udenfor dette dokument's formål og kan findes på <http://www.w3.org/TR/xmldsig-core/>.

Ved signering, anvendes xmldsig-elementet ds:Reference. ds:Reference-attributen 'URI' sættes til at pege på det element der ønskes signeret, og digest-værdien for Encoding-elementet beregnes og indsættes i elementet ds:DigestValue.

Efter godkendelse af standarden, vil der i forbindelse med udarbejdelse af skemaer, blive indsat et konkret eksempel på anvendelse af XML-Signature.

Bemærk også vedørende denne høring:

OIOXML-skemaer udarbejdes efter afsluttet høring, idet høringen kan påvirke udvalget af dataelementer (attributter) og dermed også de tilhørende OIOXML-skemaer

4. Bilag A

1.2 Anvendte typer i FESD-modellerne

FESD-modellerne er udarbejdet i UML med det formål at beskrive den logiske informationsarkitektur i en FESD-løsning.

UML-modellen er opbygget af et antal klasser, der igen er opbygget af relationer til andre klasser og primitive typer, så man kan opfatte UML-modellen som opbygget af byggesten, hvoraf den mindste er de primitive datatyper.

I UML-modellen beskriver de primitive datatyper det logiske domæne, som datatypen kan antage, men ikke hvordan den fysiske repræsentation af data skal være.

En gennemgang af de FESD-modeller, der på nuværende tidspunkt foreligger, viser, at vi har anvendt nedenstående primitive datatyper. I skemaerne ses for hver primitiv datatype, der anvendes i FESD-UML-modellen, den tilsvarende datatype for hhv. SQL og XSD.

1.2.1 integer

Benyttes til angivelse af heltal.

Der kan benyttes en angivelse af max længde – hvis intet er angivet, vil domænet være i intervallet mellem -2.147.483.648 og 2.147.483.647. Anvendte længder i den nuværende model: 2, 3, 4, 6, 8, 10.

Benyttes alene til naturlige tal (positive heltal).

Benyttes også til at danne identifikator med udfaldsrum 1 – 2000000000.

Nedenstående skema viser eksempler på heltalstyper og deres repræsentation i hhv. SQL og XSD

UML Type	Beskrivelse	SQL datatype	XSD datatype
Integer	Heltal i rummet mellem -2.147.483.648 og 2.147.483.647, begge tal inklusive. Den maksimale længde angives i modellen (*Hvordan ?*)	NUMBER(Maksimal længde)	xsd:int
NonNegativeInteger	Naturlige tal Heltal i rummet mellem 0 og 2.147.483.647, begge tal inklusive	NUMBER(Maksimal længde)	xsd:int

1.2.2 boolean

Er en grundtype i UML.

UML Type	Beskrivelse	SQL datatype	XSD datatype
Boolean	Udfaldsrummet er binært true / false (eller rigtigt / forkert).	BOOLEAN	xsd:boolean

1.2.3 Identifikationstyper

UML Type	Beskrivelse	SQL datatype	XSD datatype
URI	Enhver mulig lovlig URI. Der kan evt. anvendes en max-længde.	STRING	xsd:anyURI

HttpURI	Lovlig http(s)-adresse	STRING	xsd:anyURI Evt. restrictions der afgrænser til http.
MailToURI	Smtp-adresse på en mailmodtager.	STRING	xsd:anyURI Evt. restrictions der afgrænser til mailadresser.
UUID	Identifikator på objekt	UUID	xsd:anyURI Evt. restrictions der afgrænser til UUID.

1.2.4 char

Benyttes til karakterstrengene af varierende længde, men med en defineret maksimal længde. Anvendte længder: 1, 2, 3, 4, 15, 16, 20, 34, 40, 50, 60, 70, 110, 120, 255.

Benyttes også nogle steder til at angive en boolskværdi.

Bør ændres så typen alene bruges til tekststrengene:

UML Type	Beskrivelse	SQL datatype	XSD datatype
Char	Den minimale og maksimale længde er angivet i modellen.	VARCHAR(maksimal længde)	xsd:string Med restriction på den maximale længde
ShortText	Anvendes til felter der indeholder en kort beskrivende tekst	VARCHAR(70)	xsd:string Med restriction på den maximale længde
Text	Anvendes til en beskrivende tekst med en fast længde.	VARCHAR(255)	xsd:string Med restriction på den maximale længde
Code	Anvendes til at beskrive en kode, der er nøgle/fremmednøgle i en opslags-tabel.	VARCHAR(2)	xsd:string Med restriction på den maximale længde
Name	Anvendes til felter der indeholder navne, der kan opfattes som brugervendte nøgler.	VARCHAR(70)	xsd:string Med restriction på den maximale længde
ReferenceText	Anvendes til at felter der indeholder tekster, der af brugerne opfattes som fremmednøgler.	VARCHAR(40)	xsd:string Med restriction på den maximale længde

1.2.5 date, dateTime og time.

Typen 'Date' bruges til at angive dato.

Typen 'DateTime' bruges til 'Dato og tidspunkt', også i betydningen 'tidsstempel'.

Typen 'Time' bruges til 'klokkeslæt'.

UML Type	Beskrivelse	SQL datatype	XSD datatype
Year	Årstal	VARCHAR (4)	xsd:gYear
Date	Dato	DATE	xsd:date
DateTime	Dato og tidspunkt	DATETIME	xsd:dateTime
Time	Tidspunkt uden datoangivelse	TIME	xsd:time

1.2.6 string

Er en grundlæggende type i UML.

UML Type	Beskrivelse	SQL datatype	XSD datatype
String	Tekststreng af vilkårlig længde	STRING	xsd:string

1.2.7 float

Defineres som sådan:

UML Type	Beskrivelse	SQL datatype	XSD datatype
Float	Decimaltal hvor længde og præcision begrænses til en samlet størrelse på 16-bit.	DECIMAL(X,Y)	xsd:float