

E-BUSINESS SOLUTIONS FROM CSC

e-Tinglysningsprojektet

Løsningsspecifikation: Tværgående moduler



Dokumentoplysninger

Titel:	e-TL – Løsningsspecifikation, Tværgående Moduler
Projekt:	e-TL (Elektronisk Tinglysning)
Placering:	C:\prj\etl-doc\Documentation\TOC\05 Løsningsspecifikation – Tværgående Moduler.doc
Ikrafttrædelse:	24. april 2007
Forfatter:	Bjarne W. Hansen
Bidragydere til dokumentet:	Merete Schmidt
Godkendt af:	Domstolsstyrelsen
Fordeling:	e-TL projektet
Udskrevet:	

E-BUSINESS SOLUTIONS FROM CSC

e-Tinglysningsprojektet

Løsningsspecifikation: Tværgående moduler



Ændringslog

Version	Dato	Ændrede sider eller afsnit	Kommentarer
1.0	16.05.2007		Første udgave. Endeligt godkendt af Domstolsstyrelsen. Fremsendes til Domstolsstyrelsen

E-BUSINESS SOLUTIONS FROM CSC

e-Tinglysningsprojektet

Løsningsspecifikation: Tværgående moduler



5 Tværgående moduler

Indholdsfortegnelse

5 Tværgående moduler	1	5.9.3 Proces og Use-Cases	36
5.1 Formål	3	5.10 Anmeldte/tinglyste fuldmagter	38
5.2 Digital signatur	4	5.10.1 Indledning	38
5.2.1 Indledning	4	5.10.2 Model	39
5.2.2 X.509 Certificate standarden	4	5.10.3 Proces og Use-Cases	39
5.2.3 OCES	4	5.11 Afgiftsberegning	41
5.2.4 XML Signature i e-tinglysning	4	5.12 Hændelsesstyring	43
5.2.5 Underskrift af anmeldelser	9	5.12.1 Indledning	43
5.2.6 Anmeldelser med store bilag	10	5.12.2 Abonnementer	44
5.2.7 En eller flere underskrifter?	11	5.13 Forsendelsesmodul	46
5.2.8 Verifikation af underskrifter	11	5.13.1 Indledning	46
5.2.9 Log-on med digitalt certifikat	12	5.13.2 Overordnede services	46
5.3 Sikkerhed	13	5.13.3 Integration til print-center	48
5.3.1 Elementer i applikationssikkerhed	13	5.14 Overvågning og status	49
5.3.2 Identifikation (Authentication)	14	5.15 Statistikmodul	50
5.3.3 Adgangsrettigheder (Authorization)	17	5.15.1 Logning	50
5.4 Brugerdatatabasen	18	5.15.2 Statistiktyper	50
5.4.1 Indledning	18	5.15.3 Rettigheder	51
5.4.2 Model	19	5.15.4 Processen for etablering af statistik- og rapportmodul	51
5.4.3 Proces og Use-Cases	20	5.16 DIBS betalingssystem	52
5.5 Storkundeordning	22	5.16.1 DIBS	52
5.5.1 Indledning	22	5.16.2 Løsningsmodel	52
5.5.2 Model	22	5.16.3 Forudsætninger	52
5.5.3 Proces og Use-Cases	22	5.16.4 Betalings- og Kreditkortbetaling	52
5.6 System-system ordning	24	5.16.5 Netbankbetaling	55
5.6.1 Indledning	24	5.16.6 Onlinebetaling i den eksterne portal	55
5.6.2 Model	24	5.16.7 Betaling af tinglysningsafgift	56
5.6.3 Proces og Use-Cases	25	5.16.8 Betaling af retsafgift	58
5.7 Anmelderordning	26	5.17 Tekstfraser	59
5.7.1 Indledning	26	5.17.1 Typer af fraser	59
5.7.2 Model	27	5.17.2 Erklæring	59
5.7.3 Proces og Use-Cases	28	5.17.3 Vilkår	60
5.8 Underskriftsdatatabasen	30	5.17.4 Fuldmagtstekster	60
5.8.1 Indledning	30	5.17.5 Meddelelsetekster	60
5.8.2 Model	31	5.17.6 Standardtekster	60
5.8.3 Proces og Use-Cases	32	5.17.7 Tillægstekster	60
5.9 Fuldmagtsordningen	33	5.17.8 Opdatering	60
5.9.1 Indledning	33	5.17.9 Model	61
5.9.2 Model	34		

5.1 Formål

Løsningspecificationen for tværgående moduler har til formål at detaljere designet af enkeltstående moduler som anvendes som tværgående funktionalitet eller basale stamdata til understøttelse af de centrale tinglysningsprocesser.

5.2 Digital signatur

5.2.1 Indledning

Digital signatur i e-tinglysning er baseret på OCES X.509 certifikater samt XML Signature standarden for repræsentation af digitale underskrifter i XML.

Dette afsnit giver en oversigt over, hvordan XML Signature standarden anvendes i forbindelse med e-tinglysning til underskrift af anmeldelser, der fremsendes til tinglysningsretten.

5.2.2 X.509 Certificate standarden

Det er udenfor scope af denne beskrivelse at gennemgå X.509 standarden for digitale certifikater. De OCES certifikater, der anvendes i forbindelse med e-tinglysning, er alle baseret på standard X.509 certifikater med specifikke udvidelser, som i hovedsagen specificerer sammenknytningen mellem et certifikat og en dansk nøgle i form af et CVR nummer og/eller et CPR nummer.

X.509 standarden er beskrevet i RFC2459 (<http://www.ietf.org/rfc/rfc2459.txt>).

En overordnet gennemgang af X.509 findes på Wikipedia (<http://en.wikipedia.org/wiki/X.509>).

5.2.3 OCES

OCES certifikater er standard X.509 certifikater med udvidelser, som gør at de kan sammenknyttes med danske nøgler som CVR og CPR. Der findes 3 forskellige OCES certifikater:

1. **Virksomhedscertifikater** (VOCES) – Et generelt certifikat som kan anvendes til at identificere en virksomhed på CVR nummer.
2. **Medarbejdercertifikater** (MOCES) – Et certifikat udstedt af en virksomhed, som kan anvendes til at identificere en medarbejder eller funktion i virksomheden. Medarbejdercertifikater *kan* indeholde information om CPR nummeret på den medarbejder certifikatet er udstedt til, men gør det som udgangspunkt sjældent. Dog vil Tinglysningsretten stille krav om, at MOCES, der bruges i forbindelse med e-TL, skal indeholde CPR-nummer. CPR nummeret kan uddrages ved opslag hos certifikatudstederen (TDC).
3. **Personcertifikater** (POCES) – Personlige certifikater der indeholder en unik nøgle som ved forespørgsel hos certifikatudstederen kan oversættes til et CPR nummer.

De tekniske detaljer omkring indholdet af OCES certifikater kan ses på TDC's hjemmeside om digital signatur. (http://erhverv.tdc.dk/publish.php?dogtag=f5_e_dig_pi_tek)

5.2.4 XML Signature i e-tinglysning

5.2.4.1 XML Signature overblik

XML Signature (<http://www.w3.org/TR/xmldsig-core/>), er en generel standard for repræsentation af digitale underskrifter i XML. Standarden tillader en række forskellige måder at underskrive dokumenter på, og den angiver hvordan underskriften konkret repræsenteres som XML.

Dette afsnit beskriver XML Signature standarden ud fra e-tinglysningssystemets perspektiv.

Den overordnede opbygning af XML konstruktionen som beskrevet i XML Signature standarden er:

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
```

```
<Transforms>
  <DigestMethod>
    <DigestValue>
      </Reference>)+
</SignedInfo>
<SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
</Signature>
```

Konstruktionen repræsenteret af `<Signature>` rod elementet, udgør forståelsesmæssigt en digital underskrift af de elementer, der er udpeget via de enkelte `<Reference>` elementer.

Det som rent teknisk underskrives i XML Signature standarden er `<SignedInfo>` elementet, der indeholder de konkrete referencer til det som forståelsesmæssigt underskrives. Når man kan tale om at de elementer, der refereres til, “underskrives”, er det fordi den enkelte `<Reference>` indeholder en digest af det, der refereres til (`<DigestMethod>` og `<DigestValue>`).

Elementet `<SignatureValue>` indeholder den konkrete “værdi” af underskriften af `<SignedInfo>` elementet. Værdien kan være dannet på baggrund af forskellige algoritmer, men der tales generelt om, at underskriften er dannet ved hjælp af underskriverens private nøgle.

Underskriften kan indeholde en eller flere `<KeyInfo>` elementer. Disse elementer indeholder information om, hvordan underskriften er lavet og hvilken “offentlig nøgle”, der er anvendt ved underskriften. Informationen her kan f.eks. være et digitalt certifikat (X.509).

En typisk anvendelse af XML Signature vil være at underskrive de XML elementer, som findes i `<Object>` tag’et, men generelt kan der underskrives XML elementer placeret forskellige steder i XML dokumentet, eller der kan underskrives data, som findes eksternt i forhold til dokumentet.

5.2.4.2 Hash algoritmer

Ved underskrift af et dokument dannes en hash-værdi ud fra dokumentets indhold, uanset om det som underskrives er XML, PDF eller andet type dokument.

En hash-værdi genereres af en hash-algoritme, og fælles for alle hash-algoritmerne er, at de er en funktion, der genererer en unik nøgle (hash-værdi) ud fra et dokument. Selve hash-værdien er væsentlig mindre end selve dokumentet (typisk 128 – 512 bits).

Når man digitalt underskriver et dokument er det reelt hash-værdien man underskriver. Dette er i almindelighed nok til at bevise at man har underskrevet dokumentet. Checket kan foretages ved at sammenligne den underskrevne hash-værdi med en hash værdi man genererer ud fra dokumentet.

$$\text{hash-værdi} = \text{hash}(\text{dokument})$$

Et sådant check kan naturligvis kun foretages hvis man har det originale dokument. Dette hænger på at hash-algoritmer er en en-vejs-funktion.

Den egenskab at de enkelte hash-værdier er unikke i forhold de dokumenter, de repræsenterer, medfører, at såfremt to hash-værdier er identiske, kan man slutte, at de er genereret ud fra det samme dokument.

Dette betyder, at den mindste ændring af et dokument vil medføre, at hash-værdierne er meget forskellige. Man skal derfor være yderst forsigtig med at sikre, at dokumentet ikke ændres efter underskrift.

5.2.4.3 Kanonisering

Når man underskriver XML dokumenter, dannes der hash-værdier som beskrevet ovenfor. Kanonisering er en måde at sikre at XML dokumentet repræsenteres på den samme måde både når XML dokumentet underskrives og når signaturen checkes.

```
<etl:Anmeldelse>
  <etl:AnmeldelseDokument>
    <etl:Rolle>kreditor</etl:Rolle>
    ...
  </etl:AnmeldelseDokument>
</etl:Anmeldelse>
```

```
<etl:Anmeldelse>
  <etl:AnmeldelseDokument>
    <etl:Rolle>
      kreditor
    </etl:Rolle>
    ...
  </etl:AnmeldelseDokument>
</etl:Anmeldelse>
```

For at illustrere problemet ses herover to XML dokumenter, som ud fra et semantisk synspunkt er totalt ens, men som ville have forskellige hash-værdier.

Den eneste forskel er at værdien *kreditor* værdien i rolle tag'et har en ny line, et antal mellemrum og derefter en ny linie, mere end dokumentet i eksempel nr. 1.

Selvom *meningen* med de to dokumenter er ens, vil hash-værdien forskellig. For at imødegå disse typer af forskelle i repræsentationen af XML dokumenter anvendes en *kanoniseringsalgoritme* til at sikre, at XML'en repræsenteres ens ved underskrift samt ved check af underskriften.

I XML Signature findes en række kanoniseringsalgoritmer, som kan anvendes til at sikre, at man er enige om, hvordan XML repræsenteres.

Den kanoniseringsalgoritme, som anvendes i forbindelse med underskrift, angives i XML Signature standarden i <SignedInfo> elementet med <CanonicalizationMethod Algorithm="..." />.

De algoritmer som er mulige at anvende er:

- Kanonisk XML uden kommentarer (required)
<http://www.w3.org/TR/2001/REC-xml-c14n-20010315>
- Kanonisk XML med kommentarer (optional)
<http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>

I e-tinglysning er det besluttet at benytte den kanoniseringsmetode som ifølge XML Signature standarden er obligatorisk (kanonisk XML uden kommentarer).

5.2.4.4 Underskriftsalgoritme

Når man underskriver <SignedInfo> elementet i XML Signature standarden og dermed danner den værdi, som placeres i <SignatureValue> elementet, gøres det ved hjælp af en signeringsalgoritme.

I XML Signature standarden nævnes 2 forskellige underskriftsalgoritmer:

- DSA med SHA1 (required)
<http://www.w3.org/2000/09/xmldsig#dsa-sha1>
- RSA med SHA1 (optional)
<http://www.w3.org/2000/09/xmldsig#rsa-sha1>

Selvom standarden kræver at DSA understøttes, mens RSA er valgfri, er det valgt i første omgang kun at benytte RSA algoritmen til underskrift af anmeldelser.

Dette skyldes, at de nøgler, der er indeholdt i OCES certifikaterne, kræver anvendelse af RSA algoritmen til underskrift.

Algoritmen RSA med SHA1 kan anvendes ved underskrift af dokumenter i e-tinglysning.

Ud over de algoritmer, som er eksplicit nævnt i XML Signature standarden, findes en række nyere algoritmer med stærkere krypterings- eller hashalgoritmer. Som eksempel findes RSA algoritmer med understøttelse af hash funktioner med flere bits:

- RSA med SHA256
<http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>
- RSA med SHA512
<http://www.w3.org/2001/04/xmldsig-more#rsa-sha512>

Algoritmerne RSA med SHA256 eller SHA512 kan anvendes ved underskrift af dokumenter i e-tinglysning.

5.2.4.5 Referencer

De data, der underskrives i XML Signature standarden, udpeges gennem <Reference> elementer indeholdt i <SignedInfo> elementet.

Selve <Reference> elementet indeholder en URI attribut til at udpege et dataelement. Herudover indeholder <Reference> elementet:

- <Transforms> – specifikation af et antal transformationer, som udføres på dataelementet inden der dannes en hash-værdi til underskriften.
- <DigestMethod> – angivelse af den hash-algoritme, der anvendes til at danne hash-værdien til underskriften.
- <DigestValue> – selve hash-værdien af de data, der refereres til, efter der er udført et antal transformationer på data.

Standarden angiver en række transformationer, som kan udføres på data inden de underskrives:

- XSLT transformation (optional)
<http://www.w3.org/TR/1999/REC-xslt-19991116>
- XPath (recommended)
<http://www.w3.org/TR/1999/REC-xpath-19991116>
- Enveloped Signature (required)
<http://www.w3.org/2000/09/xmldsig#enveloped-signature>

I e-tinglysning projektet anses transformationer ikke for at bibringe løsningen yderligere forretningsmæssig værdi, og samtidig åbner transformationer op for en række problemstillinger omkring hvad der rent faktisk underskrives. Derfor er det besluttet *ikke* at tillade de nævnte transformationer. Den eneste “transformation”, der tillades anvendt, er kanonisering, som er beskrevet tidligere i dette dokument.

XML Signature standarden har en krævet digest algoritme (hash-algoritme) til brug for generering af hash-værdien for de data, som underskrives (SHA1), og derudover er der defineret yderligere digest algoritmer i standarden for XML Encryption. Det drejer sig om:

- SHA1 (<http://www.w3.org/2000/09/xmldsig#sha1>)
- SHA256 (<http://www.w3.org/2001/04/xmlenc#sha256>)
- SHA512 (<http://www.w3.org/2001/04/xmlenc#sha512>)

Digest algoritmerne SHA1, SHA256 og SHA512 tillades alle til dannelse af digests i forbindelse med signering af dokumenter i e-tinglysning.

De URI'er, der anvendes til at udpege et dataelement, som skal underskrives, kan antage forskellige former i henhold til XML Signature standarden:

- "" (tom streng) – refererer til hele det dokument `<Signature>` elementet er indeholdt i. Denne facilitet anvendes ikke i e-tinglysning – se beskrivelsen af opbygning og signering af anmeldelser i de efterfølgende afsnit.
- "#id-på-xml-element" – tillader reference til et XML element med id = "id-på-xml-element", som findes et eller andet sted i det dokument som indeholder signaturen. Denne facilitet anvendes i e-tinglysning til at udpege selve anmeldelsesdokumentet, samt eventuelle bilag indlejret i anmeldelsen. Se beskrivelsen af opbygning og signering af anmeldelser i de efterfølgende afsnit.
- "http://example.com/data/test.xml" – URI reference til eksterne data, der er underskrevet som en del af den digitale signatur. XML Signature standarden *anbefaler*, at der tillades brug af HTTP URL'er ved referencer til eksterne data. I e-tinglysning vil der være mulighed for anvendelsen af HTTP baserede URI'er i begrænset omfang. (Se afsnit 5.2.6 "Anmeldelser med store bilag" for yderligere information)
- XPath/Pointer udtryk – Disse udtryk tillades i XML Signature standarden til udpegning af det XML element som underskrives. I første release af e-tinglysning understøttes disse ikke.

Sammenfattende er der i e-tinglysning valgt en simpel pragmatisk løsning for referencer til de data som underskrives i anmeldelse. De valgte måder at referere data på dækker de umiddelbare forretningsmæssige behov i e-tinglysning.

Valgene udelukker på ingen måde en fremtidig indførelse af nye måder at referere på.

5.2.4.6 Nøgleinformation

Elementet `<KeyInfo>` indeholder i XML Signature standarden information om den eller de nøgler, der er anvendt ved underskrift af `<SignedInfo>` elementet.

Standarden udpeger et antal nøgle informationer der kan være indeholdt:

- <http://www.w3.org/2000/09/xmldsig#DSAKeyValue>
- <http://www.w3.org/2000/09/xmldsig#RSAKeyValue>
- <http://www.w3.org/2000/09/xmldsig#X509Data>
- <http://www.w3.org/2000/09/xmldsig#PGPData>
- <http://www.w3.org/2000/09/xmldsig#SPKIData>
- <http://www.w3.org/2000/09/xmldsig#MgmtData>

Da underskrifter i e-tinglysning er baseret på anvendelsen af OCES certifikater, eller X.509 certifikater i al almindelighed, er det valgt at indholdet i `<KeyInfo>` elementet er X509Data.

5.2.4.7 Sammendrag

Nedenfor er de valg af algoritmer og datarepræsentation, der er taget i forbindelse med e-tinglysningsprojektet, i forhold til XML Signature standarden dokumenteret i tabelform.

Egenskab	Valg i e-tinglysning
CanonicalizationMetod	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
SignatureMethod	http://www.w3.org/2000/09/xmldsig#rsa-sha1

	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1 http://www.w3.org/2001/04/xmlenc#sha256 http://www.w3.org/2001/04/xmlenc#sha512
KeyInfo	http://www.w3.org/2000/09/xmldsig#X509Data

5.2.5 Underskrift af anmeldelser

XML Signature standarden anvendes til underskrift af enkeltstående anmeldelser og til anmeldelser indeholdt i en kuvertordning. De underskriftstekniske metoder og algoritmer er beskrevet i ovenstående afsnit.

Ved dannelse af en digital underskrift af en anmeldelse vil den overordnede struktur af anmeldelsen være som følger:

```
<etl:Anmeldelse>
  <etl:AnmeldelseDokument id="dokument">
    ...
  </etl:AnmeldelseDokument>

  <etl:AttachmentBinaryData id="bilag1" ... />
  <etl:AttachmentBinaryData id="bilag2" ... />
  ...
  <etl:Underskrifter>
    <ds:Signature ... />
    <ds:Signature ... />
    ...
  </etl:Underskrifter>
</etl:Anmeldelse>
```

Konkret indeholder anmeldelsen altså selve det anmeldelsesdokument, der repræsenterer data som er en del af den tinglysningsmæssige transaktion, de bilag som evt. er vedhæftet anmeldelsen, samt underskrifter af anmeldelsesdokumentet og eventuelle bilag.

Selve anmeldelsesdokumentet er altid indlejret som XML i anmeldelsen, og refereres fra <Reference> elementet ved brug af ID URI (for eksemplet ovenfor vil URI referencen være URI="#dokument").

Bilag til anmeldelsesdokumentet kan indlejres i anmeldelsen som base64 encoded data. Hvis et bilag indlejres i dokumentet refereres det via ID URI på samme måde som der refereres til anmeldelsesdokumentet, f.eks. URI="#bilag1".

Indlejring af større bilag kan være u hensigtsmæssig i forhold til performance og driftsstabilitet af e-tinglysningsystemet. Af den grund vil der blive sat en grænse for størrelsen af anmeldelsen, inklusiv alle bilag.

Næsten uanset den konkrete valgte grænse for størrelsen af bilag, som indlejres i anmeldelsen, kan der i e-tinglysning opstå behov for at kunne indsende anmeldelser med bilag som er specielt store. Til det formål designes e-tinglysningsystemet til at kunne håndtere bilag, som ikke nødvendigvis fremsendes sammen med anmeldelse – men som er underskrevet som en del af anmeldelsen. Se afsnittet "Anmeldelser med store bilag" for yderligere information.

Konstruktionen i forbindelse med kuvertordningen er i princippet ikke anderledes end for den enkelte anmeldelse. Kuverten kan indeholde en eller flere anmeldelser samt en følgeseddel.

De enkelte anmeldelser i kuverten skal være underskrevet som vist ovenfor, men kuverten indeholde en underskrift af følgesedlen.

```
<etl:Kuvert>
  <etl:Anmeldelse ... />
  <etl:Anmeldelse ... />
  <etl:Følgeseddel ... />
  ...
  <etl:Underskrifter>
    <ds:Signature ... />
  </etl:Underskrifter>
</etl:Kuvert>
```

Underskriften af følgesedlen dannes af den part, der indsender kuverten, evt. på vegne af en eller flere anmeldere. Underskriften af følgesedlen er alene en dokumentation for, at man ønsker de anmeldelser, som er indeholdt i kuverten, behandlet i henhold til følgesedlens indhold.

5.2.6 Anmeldelser med store bilag

For at begrænse størrelsen af de enkelte anmeldelser, vil der i e-tinglysningsystemet blive sat en begrænsning på den samlede størrelse af de bilag, der indsendes sammen med en anmeldelse. Dette sker for at sikre performance og driftstabilitet af modtagelsesprocessen i e-tinglysning.

For at understøtte de situationer hvor en anmelder specifikt har brug for at vedhæfte store dokumenter, vil der blive implementeret en mulighed for at indsende disse bilag på forhånd, hvorefter der kan refereres til dem i den digitale underskrift.

For at indsende et bilag kaldes en Web Service på e-tinglysningsystemet (BilagIndsend) med bilaget og angivelse af en digest algoritme som parameter.

E-tinglysningsystemet vil oprette dette dokument i dokumentdatabasen og tildele det et unikt id samt en URI, der kan anvendes til at referere til dokumentet. Ligeledes vil e-tinglysningsystemet beregne en digest af dokumentet i henhold til den specificerede digest algoritme.

Resultatet af Web Service kaldet er, at det kaldende system får information tilbage om den tildelte UUID samt en digest beregnet af e-tinglysningsystemet. Der anvendes de samme digest algoritmer ved indsendelse af store bilag, som der anvendes ved underskrift af anmeldelser. Den unikke identifikation returneres som en URN på formen "urn:uuid:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx" i overensstemmelse med retningslinierne i "Unikke Identifikatorer til digitale

objekter" fra IT- og Telestyrelsen

(<http://www.oio.dk/dataudveksling/fora?o=1b88b77c7e1b458c2824d1f6a0a3b8b0>).

Det kaldende system bør sammenligne den returnerede digest med en digest systemet selv har beregnet, for at sikre at der er enighed om, at der refereres til det samme dokument.

Den returnerede URN placeres i URI attributten på <Reference> elementet i signaturen, den benyttede digest algoritme angives i <DigestMethod> elementet og den returnerede digest placeres i <DigestValue> elementet. Den samlede <SignatureInfo> i <Signature> elementet underskrives herefter som for øvrige anmeldelser.

Når e-tinglysning modtager anmeldelsen, vil den i dokumentdatabasen kunne fremfinde det i forvejen indsendte bilag på baggrund af URI referencen i den digitale underskrift.

Bemærk at ovenstående fremgangsmåde tillader en anmelder at indsende flere anmeldelser med reference til det samme dokument. Dette sker ved at genbruge den URI og digest som blev returneret af e-tinglysning. Dette kan anvendes til at vedhæfte enslydende dokumenter til flere anmeldelser - f.eks. standard forretningsbetingelser eller lignende.

Der stilles ikke krav fra e-tinglysning om, at ens bilag refereres via samme bilagsreference, men hvis funktionaliteten anvendes, mindskes behovet for kapacitet i tinglysningsystemet, ligesomt anmeldere ikke behøver at indsende enslydende dokumenter flere gange.

5.2.7 En eller flere underskrifter?

I forbindelse med dannelsen af en underskrift kan man som underskriver vælge forskellige måder at underskrive flere elementer i en anmeldelse på. Der er hovedsageligt tale om to forskellige muligheder, der kan kombineres på forskellige måder.

1. *Der dannes en underskrift (<ds:signature>) for hvert element (reference) man ønsker at underskrive.*
Dette tillader, at hvert element underskrives uafhængigt af andre elementer i anmeldelsen, hvilket kan tillade en vis fleksibilitet, hvis anmeldelser/dokumenter fremsendes mellem forskellige parter inden anmeldelse til Tinglysningsretten.
2. *Der dannes en underskrift (<ds:signature>) for et antal elementer (reference) på en gang.*
Denne fremgangsmåde underskriver et antal elementer "samlet". Således kan enkelt elementer ikke tages ud af anmeldelsen uden at bryde signaturen.

Om der anvendes den ene eller den anden fremgangsmåde afhænger af, hvad man ønsker at opnå med underskriften.

Normalt vil man ønske at underskrive en anmeldelse samlet, således at anmeldelsesdokumentet samt eventuelle bilag ikke kan opsplittes af en tredjepart. Således vil vedkommende, som modtager anmeldelsen, alene kunne tilføje sin egen signatur til anmeldelsen.

Omvendt vil man måske fremsende en anmeldelse til tredjepart, som indeholder de elementer, der skal fremsendes til tinglysning, med en samlet underskrift, og derudover et bilag, som er signeret separat. Dette bilag kan af tredjepart tages ud af anmeldelsen inden den indsendes til tinglysningsretten.

E-tinglysningsystemet understøtter begge fremgangsmåder til generering af digitale signaturer og kan modtage signaturer baseret på begge fremgangsmåder.

5.2.8 Verifikation af underskrifter

Når en digital signatur anvendes til underskrift eller login i e-tinglysningsystemet checkes certifikatet og derefter underskriften. Dette gøres umiddelbart ved modtagelse af en anmeldelse og ved login.

Senere i tinglysningsprocessen vil e-tinglysningsystemet checke dispositionsretten i forhold til de registreringer, som findes i e-Akten. Disse check er ikke en del af verifikationen af den digitale underskrift, men forretningslogik hørende til tinglysningsprocessen.

Verifikation af certifikatet består af:

- Verifikation af udstederen af certifikatet
- Validering af at certifikatet ikke er udløbet
- Validering af at certifikatet ikke er spærret gennem CRL eller via OCSP
- Indhentning af CPR nummer for brugere, der anvender privat OCES certifikat
- Indhentning af CPR nummer på medarbejdere, der har registreret CPR-nummer i medarbejdercertifikatet
- CVR nummeret står i klartekst i certifikatet og uddrages derfor direkte af certifikatet (virksomheds- og medarbejdercertifikater)

Når verifikationen af det anvendte certifikat er gennemført checkes den digitale signatur

- Alle referencers digest i <DigestValue> elementet checkes
- Der beregnes en digest over <SignedInfo> elementet

- Værdien i <SignedValue> dekrypteres med den offentlige nøgle fra det certifikat, som blev anvendt til underskrift, og sammenlignes med den beregnede digest for <SignedValue> elementet.

I e-tinglysningsystemet opbevares resultatet af verifikationen for fremtidig reference.

Bemærk, at verifikationsprocessen *ikke* vil afvise en anmeldelse straks, blot fordi verifikationen af et certifikat fejler. Hvis et certifikat er udløbet, spærret eller hvis personen er registreret som død i CPR, vil anmeldelsen fortsætte i tinglysningsprocessen, men vil blive udtaget til manuel behandling.

5.2.9 Log-on med digitalt certifikat

Adgangskontrol baseret på et OCES certifikat opnås ved at anvende OpenLogon komponenten fra OpenOCES, samt komponenter på portal serveren til validering af log-on.

Princippet for en sådan adgangskontrol adskiller sig ikke væsentlig for beskrivelsen af digital signatur i afsnittene ovenfor, idet adgangskontrol består i, at man beder den, som ønsker adgang, om at underskrive en lille stump information med sit digitale certifikat, hvorefter man validerer signaturen.

Som ved validering af underskrifter for digitale underskrifter, checkes det anvendte certifikat for at sikre at dette er gyldigt. Dernæst uddrages de sædvanlige informationer i form af CPR/CVR nummer etc.

De rettigheder en bruger besidder efter log-on er baseret på roller som tildeles i forbindelse med log-on samt eventuelle registreringer om brugeren, der er foretaget i e-tinglysningsystemet. For yderligere information henvises til afsnittet om sikkerhed.

5.3 Sikkerhed

Dette afsnit beskriver arkitekturen for applikationssikkerheden i e-tinglysningsystemet. Ved applikationssikkerhed forstås den arkitektur og de mekanismer, der implementeres som en del af løsningen for at opretholde og understøtte sikkerhed i portalen og e-tinglysningsmotoren.

Generelt består en fuldstændig beskrivelse af sikkerhed af flere elementer end det, som blot dækker den/de applikationer, der indgår i løsningen. Ofte beskrives også elementer som fysisk sikkerhed, driftstabilitet, “disaster recovery”, “denial-of-service” og andre lignende aspekter ved den samlede sikkerhed. Disse områder dækkes ikke i dette afsnit, der alene fokuserer på sikkerhed fra applikationsarkitektur perspektivet.

5.3.1 Elementer i applikationssikkerhed

Den samlede applikationssikkerhed består af forskellige elementer, som tilsammen udgør sikkerhedsarkitekturen. Disse elementer spiller hver deres specifikke rolle i den samlede sikkerhedsløsning.

Sikkerhedssystemer baseres normalt på *roller*, således at de *rettigheder* en given bruger har afgøres ud fra hvilke *roller* vedkommende optræder i. Dette sker bl.a. for at lette den administrative byrde omkring tildeling og fjernelse af rettigheder.

Bemærk! De roller som omtales her er **ikke** de tinglysningsmæssige roller, der anvendes i forbindelse med en anmeldelse, men i stedet tekniske roller, som anvendes i forbindelse med opbygning af sikkerhedsarkitekturen. De tekniske roller benævnes **bruger roller**.

For at systemet skal kunne bestemme hvilke brugerroller – og dermed hvilke rettigheder – en bruger besidder, skal systemet ved enhver tilgang etablere nogle fakta omkring brugere.

Først og fremmest skal brugeren kunne identificeres til et acceptabelt niveau – man skal med andre ord vide hvem brugeren er. Dette sker gennem hvad der normalt kaldes identifikation (*authentication*). Den meste almindelige identifikationsmekanisme kendes fra brugernavn/password.

Dernæst skal systemet på baggrund af brugerens identitet fastslå, hvilke brugerroller brugeren er medlem af. Dette sker typisk ved at brugeren gennem sikkerhedssystemet defineres til at tilhøre et konkret antal grupper/brugerroller, men det kan også ske på baggrund af andre mekanismer. Et eksempel på andre mekanismer kan f.eks. være de OCES certifikater, der anvendes i e-tinglysningsløsningen. På baggrund af OCES certifikattypen kunne en bruger f.eks. tildeles brugerrollerne *Privat*, *Medarbejder* eller *Virksomhed*.

Når identitet og brugerroller er fastslået, vil en applikation kunne tildele konkrete rettigheder til at udføre en eller flere handlinger i systemet. Dette benævnes normalt *authorization*.

Rettigheder kan evalueres på mange forskellige måder. Ofte sker det ved, at en brugerrolle beskriver om en rettighed er tilgængelig eller ej – altså en slags ja/nej situation. F.eks. kan applikationen spørge autorisationssystemet, om en bruger må oprette, rette eller slette en konkret entitet i databasen.

Ud over de simple rettighedscheck findes der mere komplekse måder at afgøre en rettighed på. F.eks. vil man i e-tinglysnings have brug for at checke mod Erhvervs- og Selskabsstyrelsen hvorvidt en person har lov til at underskrive salget af en ejendom. Disse rettigheder kan være sammensatte, således at der f.eks. kræves mere end én underskrift.

5.3.2 Identifikation (Authentication)

5.3.2.1 Ekstern portal

Visse dele af den eksterne portal kræver ingen specifikke rettigheder, og enhver kan dermed tilgå disse sider på portalen. Sådanne brugere, som ikke har identificeret sig overfor portalen, besidder brugerrollen *anonym*.

De sider, der kræver at brugeren er kendt af tinglysningssystemet, f.eks. oprettelsen af en anmeldelse, vil kræve at brugeren besidder en eller flere brugerroller over *anonym* niveauet. For at tildele disse brugerroller bliver brugeren bedt om at logge ind med sit digitale certifikat.

Dette sker gennem brug af komponenten *OpenLogon* der anvender et OCES certifikat til at underskrive en lille log-in meddelelse, der kan valideres af e-tinglysning portalen.

På baggrund af certifikatet tildeles brugeren en af følgende brugerroller:

- **Person** – en bruger der er logget ind med et personligt OCES certifikat. Ud over brugerrollen vil systemet kende CPR nummeret på den aktuelle bruger
- **Medarbejder** – en bruger der har identificeret sig med et OCES medarbejdercertifikat. Ud over brugerrollen vil systemet kende virksomhedens CVR nummer samt en unik nøgle for medarbejderen, som f.eks. kan være et personalenummer. OCES medarbejdercertifikater skal tillige indeholde CPR nummer på medarbejderen.
- **Virksomhed** – en bruger der har identificeret sig med et OCES virksomhedscertifikat. Ud over brugerrollen kender systemet virksomhedens CVR nummer samt et unikt løbnummer for certifikatet (en virksomhed kan have flere virksomhedscertifikater).

Denne del af processen varetages af en speciel OCES *Authentication Provider* fra Signaturgruppen. En *Authentication Provider* er en speciel komponent, som kan konfigureres ind i BEA infrastrukturen til at foretage identifikation (authentication).

På denne måde har vi inddelt alle brugere i 3 forskellige brugerroller.

Alle privatpersoner kan forespørge, anmelde og tilgå egne informationer under behørig hensyntagen til betaling af afgifter. Dermed kræves der ikke yderligere identifikation eller rolletildeling for privatpersoner, der tilgår den eksterne portal.

Med hensyn til brugere, der tilgår portalen på vegne af en arbejdsgiver, dvs. ved brug af medarbejder eller virksomhedscertifikat, forholder det sig lidt anderledes. Visse handlinger som udføres på vegne af virksomheder eller myndigheder kræver yderligere tildeling af rettigheder. Yderligere rettigheder etableres gennem brugerroller ud over de 3 basale brugerroller (*person*, *medarbejder* og *virksomhed*).

For at etablere denne yderligere identifikation af en konkret brugers brugerroller – og dermed i sidste ende hvilke rettigheder brugeren har – anvendes de informationer, der er registreret for konkrete certifikater i *brugerdatabasen* (se 5.4 Brugerdatabasen). Information i brugerdatabasen vedligeholdes af virksomheden selv, gennem en eller flere udpegede administratorer. Det er dermed virksomhedens eget ansvar, hvilke brugerroller dens medarbejdere må antage på virksomhedens vegne.

De konkrete brugerroller, der kan tildeles medarbejdere, er ikke præcist fastlagt.

Der findes andre interessenter, der ligeledes kan tilgå den eksterne portal med specielle rettigheder. Det drejer sig f.eks. om *fogedretten*, *skifteretten*, *SKAT*, *kommuner*, *landinspektører* etc.

Disse skal som beskrevet for virksomheder ovenfor tildele specifikke medarbejdere adgang til på deres vegne at varetage opgaver i tinglysningsystemet. Dette gøres efter samme opskrift som for virksomheder gennem *brugerdatabasen*, blot vil disse kunne tildele deres medarbejdere et andet sæt af brugerroller.

Processen med at fastlægge brugerroller – ud over de roller, som kan etableres ud fra certifikater – sker gennem en såkaldt *Role Mapping Provider*. Role Mapping Provideren tildeler brugerroller

baseret på den information, som findes i det certifikat, som blev anvendt ifbm. login sammenholdt med den information, som findes i *brugerdatabasen*.

5.3.2.2 Intern portal

For den interne portal er der i kravspecifikationen angivet krav om sammenhæng med Tinglysningsrettens Microsoft Active Directory, således at der opnås single-sign-on mellem e-tinglysning applikationen (den interne portal) og brugerens Windows login.

Denne integration kan realiseres ved at anvende en *Authentication Provider* i BEA portalen som etablerer netop denne integration. Denne Authentication Provider vil konkret anvende SPNEGO protokollen til at etablere sammenhæng mellem Windows brugeren og den sikkerhedskontekst som repræsenterer brugeren i den interne portal.

Tildelingen af brugerroller til de interne medarbejdere sker derefter ved at en konkret *Role Mapping Provider* tildeler brugeren en eller flere af de brugerroller, der er tildelt brugeren i Microsoft Active Directory.

De konkrete brugerroller for en tinglysningsmedarbejder vedligeholdes dermed gennem den almindelige administrative brugergrænseflade for Microsoft Active Directory.

5.3.2.3 System-system adgang

De handlinger, der kan foretages ved system-system kommunikation, svarer på overordnet niveau til de handlinger, som kan foretages ved anvendelse af den eksterne portal. Dermed opstår i princippet det samme behov for identifikation, tildeling af brugerroller og autorisation, som det er tilfældet for portalen.

Et specielt forhold i den forbindelse er dog, at det hos den eksterne interessent vil være en server, som kommunikerer med tinglysningssystemet på vegne af en bruger eller et andet system hos den eksterne interessent.

Fra et tinglysningsperspektiv vil dispositionsret i forhold til anmeldelser alene blive afgjort af de underskrifter, der forefindes i selve anmeldelsen som indsendes. For anmeldelser er der således ikke behov for yderligere identifikation.

For forespørgsler og andre typer af opslag i e-tinglysning systemet vil der dog være behov for identifikation til et overordnet virksomhedsniveau. Således behøver tinglysningssystemet ikke nødvendigvis at kende den præcise identitet på brugeren. Systemet skal alene have kendskab til hvilken virksomhed forespørgslen kom fra.

For visse administrative opgaver, som f.eks. vedligehold af brugerdatabasen, anmelderordningen og underskriftsdatabasen, vil tinglysningssystemet dog have brug for at kende den præcise identitet på den bruger, som tilgår systemet (administratoren). Administration af en virksomheds opsætning i e-tinglysningssystemet vil i første version foregå gennem den eksterne portal. Senere vil der muligvis blive åbnet op for at administration af en virksomhed kan ske gennem system-system kald.

Identifikation (authentication) vil for system-system kald skulle ske sammen med de Web Service kald, der udgør kommunikationen. Til dette brug anvendes standarden WS-Security, som tillader den kaldende part at medsende information om sig selv, eller den bruger som systemet repræsenterer.

WS-Security standarden tillader, at der anvendes elementer fra XML Signature standarden til at sikre identitet af afsenderen (*authentication*) samt integritet af beskeden (*integrity*).

Ud over identitet (af afsender) og integritet (af beskeden) tales der om konfidentialitet (af indholdet af beskeden). Konfidentialitet (*confidentiality*) opnås gennem kryptering af transportkanalen eller ved kryptering af den enkelte besked.

I e-tinglysning anvendes HTTPS protokollen til kommunikation mellem den enkelte system-system bruger. HTTPS etablerer en krypteret "tunnel" hvor igennem kommunikationen foregår, og der er derfor som udgangspunkt ikke behov for yderligere kryptering.

```

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="..." xmlns:wssse="..." xmlns:wssu="..." xmlns:ds="...">
  <soap:Header>
    <wssse:Security>
      <wssse:BinarySecurityToken ValueType="..." EncodingType="..." wssu:Id="X509Token">
        MIIeZzCCA9CgAwIBAgIQEmtJZc0rqrKh5i...
      </wssse:BinarySecurityToken>

      <ds:Signature>
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="..." />
          <ds:SignatureMethod Algorithm="..." />
          <ds:Reference URI="#body">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <ds:DigestValue>EULddytSol...</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
          BL8jdfToEb1l/vXcMZNNjPOV...
        </ds:SignatureValue>

        <ds:KeyInfo>
          <wssse:SecurityTokenReference>
            <wssse:Reference URI="#X509Token" />
          </wssse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wssse:Security>
  </soap:Header>

  <soap:Body wssu:Id="body">
    ...
  </soap:Body>
</soap:Envelope>

```

Figur 1: SOAP kald med WS-Security header

Eksemplet i figur 1 ovenfor skitserer et SOAP kald hvor WS-Security standarden anvendes til at etablere sikkerhed for, at den som kalder den konkrete service er autoriseret til denne type system-system tilgang.

Med udgangspunkt i beskrivelsen af hvordan XML Signature standarden anvendes i forbindelse med e-tinglysning er anvendelsen af WS-Security blot et spørgsmål om at "genkende" brugen af XML Signature standarden, samt nogle få WS-Security specifikke forhold.

Først og fremmest konstateres det at WS-Security elementet (<wssse:Security>) placeres i SOAP header for kaldet.

Det første delement (<wssse:BinarySecurityToken>) angiver det sikkerhedselement, som anvendes til etablering af identitet og integritet - i dette tilfælde et X.509 certifikat. I e-tinglysning anvendes X.509 certifikater i forbindelse med WS-Security, da denne teknologi i forvejen anvendes i forbindelse med underskrift af anmeldelser. I princippet behøver vi ikke her at kræve at der anvendes OCES X.509 certifikater, men det vil som udgangspunkt være det letteste.

Herefter indeholder WS-Security elementet en mere eller mindre standard XML Signature blok, der udpeger og underskriver indholdet af SOAP body elementet. Således underskrives SOAP body elementet efter samme principper som vi underskriver anmeldelser.

Den eneste “specialitet” i forhold til WS-Security er, at der fra XML Signature elementet `<ds:KeyInfo>` refereres til det oprindelige sikkerheds token placeret i `<wsse:BinarySecurityToken>` elementet, frem for blot at inkludere X.509 certifikatet her.

Fra serverens perspektiv vil vi altså kende underskriveren af service kaldet (Web Service), på samme måde som vi kender underskrivere af anmeldelserne. På samme måde som certifikatet for en underskriver på en anmeldelse checkes for gyldighed, checkes også certifikatet anvendt til underskrift af SOAP-kaldet.

Efter at have konstateret at certifikatet er gyldigt, checkes det, at der er tale om et certifikat, der tilhører en virksomhed registreret i system-system ordningen hos Tinglysningsretten. Dette sker for at kun autoriserede system-system brugere kalder Web Services hos e-tinglysning.

5.3.3 Adgangsrettigheder (Authorization)

Med adgangsrettigheder forstås den enkelte brugers konkrete mulighed for at tilgå eller udføre en specifik handling i e-tinglysningssystemet. Brugeren checkes således konstant for hvorvidt vedkommende har autorisation til at udføre de handlinger vedkommende foretager på portalen eller via system-system kald.

Disse autorisationscheck udføres konstant af det programmel, som udgør de enkelte forretningsservices, samt det programmel, der udgør portalerne.

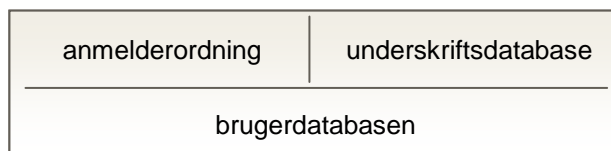
Den konkrete evaluering af hvorvidt en bruger har ret til at udføre en given handling, sker ofte på baggrund af den/de *brugerroller* brugeren er blevet tildelt i forbindelse med identifikation (authentication). Således konfigureres der i e-tinglysningssystemet en sammenhæng mellem *handlinger* og *brugerroller*.

Denne sammenknytning og konfiguration kan opsættes i sikkerhedssystemet i BEA infrastrukturkomponenterne.

En række rettigheder i systemet kan *ikke* evalueres simpelt på baggrund af en brugerrolle tildelt i forbindelse med identifikation af brugeren. Dette gælder rettigheder, der baserer sig på dynamiske forhold eller konkrete registreringer i de interne eller eksterne systemer.

Således udgør *brugerdatabase*, *anmelderordningen* og *underskriftsdatabase* eksempler på registreringer lokalt i e-tinglysningssystemet, der påvirker den konkrete brugers rettigheder i systemet. Specielt for *underskriftsdatabase* gælder der, at visse rettigheder i e-tinglysningssystemet er baseret på informationer, der opbevares uden for Tinglysningsretten, nemlig hos Erhvervs- og Selskabsstyrelsen.

Registreringer i brugerdatabase, anmelderordningen og underskriftsdatabase udgør et rettmæssigt hierarki. Således skal en bruger (identificeret ved et certifikat) være registreret i brugerdatabase for at kunne optræde under anmelderordningen og underskriftsdatabase.



Bemærk! Registrering i brugerdatabase og andre rettighedsregistrerende databaser er kun nødvendig for brugere, der skal besidde specielle rettigheder i forhold til e-tinglysningssystemet.

Brugerdatabase, storkundeordning, system-system ordning, anmelderordning og underskriftsdatabase er beskrevet yderligere i de efterfølgende afsnit.

For at håndtere disse *dynamiske* rettigheder implementeres en komponent til sikkerhedssystemet, som muliggør evaluering af disse typer af rettigheder. Denne type komponenter betegnes typisk *Authorization Providers*.

5.4 Brugerdatatabasen

5.4.1 Indledning

For privates brug af e-tinglysning kan brugerroller og rettigheder afgøres alene ud fra deres anvendelse af deres personlige OCES certifikat samt de registreringer, der findes i e-tinglysningssystemets akt database. En bruger der tilgår e-tinglysningssystemet med sit personlige OCES certifikat tildeles brugerrollen *person*.

Personer der tilgår e-tinglysningssystemet med medarbejder- eller virksomhedscertifikat, tildeles som udgangspunkt brugerrollen *medarbejder* eller *virksomhed*. Disse roller åbner op for brugerens basale anvendelse af e-tinglysningssystemet.

En række andre anvendelser af e-tinglysning kræver, at en konkret bruger besidder et antal yderligere brugerroller ud over den brugerrolle, som kan uddrages af hvilket OCES certifikat, der anvendes til identifikation af brugeren.

Således vil der for en virksomhed kunne registreres særlige egenskaber, som regulerer virksomhedens – og dens ansattes – brug af e-tinglysningssystemet.

Eksempler på sådanne specielle registreringer omfatter f.eks.:

- Virksomhedens status i forhold til storkundeordningen
- Virksomhedens status i forhold til anvendelse af system-system ordningen
- Virksomhedens status i forhold til at benytte den særlige anmelderordning, samt regler for virksomhedens ansattes brug af denne ordning
- Virksomhedens registrering af specifikke ansatte til at kunne tegne virksomheden i underskriftsdatatabasen

Alle disse registreringer i forhold til en virksomheds brug af e-tinglysningssystemet hægtes op på en central registrering af virksomheden, samt eventuelt registrering af visse medarbejdere i virksomheden.

Det er derfor ikke påkrævet at en virksomhed registrerer alle ansatte som tilgår e-tinglysningssystemet, men blot de ansatte som indtager specielle rettigheder på vegne af virksomheden.

Ud over de mest almindelige registreringer beskrevet ovenfor, kræves der et antal specielle rettigheder for brugere, der tilhører bestemte typer af virksomheder og myndigheder. Dette gælder for medarbejdere ved SKAT, medarbejdere i foged- og skifteretten etc.

Disse medarbejdere vil ikke have medarbejder- eller virksomhedscertifikater, som skiller sig ud fra den type certifikater, der udstedes til andre typer virksomheder. Derfor er det nødvendigt i e-tinglysningssystemet at registrere specifikke brugerroller for disse "specielle" medarbejdere.

Formålet med "Brugerdatatabasen" bliver således at lave en sammenknytning mellem virksomheder og disses medarbejdere, samt muliggøre, at der tildeles specifikke brugerroller til disse medarbejdere.

Administrationen af disse registreringer sker til dels af Tinglysningsretten og til dels af de enkelte virksomheder selv gennem virksomhedens administratorer.

Bemærk! Denne facilitet i e-tinglysning tillader registrering af konkrete certifikater for personer, medarbejdere og virksomheder som skal have specielle adgangsrettigheder til e-tinglysning. Den vil dermed blive en del af *authentication* og *authorization* delen af sikkerhedssystemet i e-tinglysning. Se også afsnittet vedrørende sikkerhed (5.3 "Sikkerhed").

I e-tinglysning brugerdatatabasen registreres således de *certifikater* som virksomheden tillader anvendes i forbindelse med tinglysning. Når der tales om *certifikater* frem for *medarbejdere* skyldes

det, at der kan være tale om både virksomhedscertifikater og medarbejdercertifikater, og at en eventuel sammenknytning mellem et certifikat og en konkret medarbejder alene bestemmes af den virksomhed, som udsteder certifikaterne.

Brugerdata-basen vedligeholdes af den enkelte virksomhed selv, gennem en eller flere godkendte administratorer identificeret ved et certifikat per administrator. De administratorer, som vedligeholder brugerdata-basen på vegne af en virksomhed kan f.eks. være dem som i forvejen er udnævnt som *LRA (Local Registration Authority)* i forhold til oprettelsen af OCES medarbejdercertifikater for virksomheden.

Hvis en person anvender virksomheds- eller medarbejdercertifikat på den eksterne portal, vil det ved log-in blive kontrolleret hvilke rettigheder certifikatet giver i forhold til anvendelse på portalen.

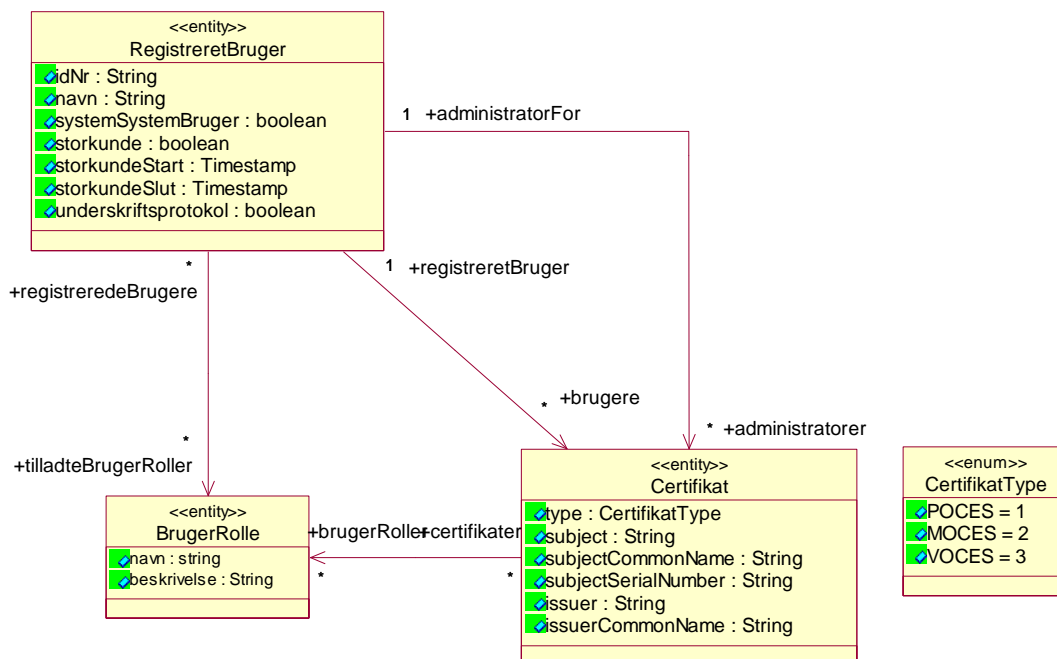
Bemærk! Registrering af et certifikat i brugerdata-basen åbner alene op for tildelingen af basale brugerroller i forbindelse med identifikation af brugeren. Registrering ændrer ikke på, om certifikatet kan anvendes til at disponere på virksomhedens vegne (underskriftsdata-basen) eller om det kan anvendes til at træde i stedet for en anden disponents underskrift (anmelderordningen).

Der vil være et sammenfald mellem de certifikater, som registreres i brugerdata-basen med de som optræder i underskriftsdata-basen og de anmelderordninger, som er oprettet for en given virksomhed. Således vil konfiguration og vedligehold af opsætning for underskriftsdata-basen og anmelderordninger tage udgangspunkt i de certifikater som er registreret i brugerdata-basen.

Anmelderordningen og underskriftsdata-basen beskrives i det efterfølgende afsnit.

5.4.2 Model

5.4.2.1 UML



5.4.2.2 Beskrivelse

Modellen tager udgangspunkt i klassen `RegistreretBruger`, som repræsenterer en virksomhed eller myndighed, der kan tilgå e-tinglysningsystemet.

En registreret bruger identificeres ved idNr attributten, der for danske virksomheder vil være virksomhedens CVR nummer, mens evt. udenlandske virksomheder vil være identificeret gennem anden nøgle.

Ud over identifikationsnøglen indeholder RegistreretBruger attributten navn, der for danske virksomheder vil være det navn som virksomheden kendes under i CVR, mens det for udenlandske virksomheder vil være det navn virksomheden blev oprettet under hos tinglysningsretten.

Hver RegistreretBruger kan gennem to forskellige relationer referere til et antal objekter af typen Certifikat.

Relationen administratorer (1:n) udpeger et antal Certifikat objekter som kan anvendes af virksomheden i forbindelse med administration af brugerdata-basen, mens relationen brugere (1:n) udpeger Certifikat objekter, der kan benyttes ved særlige handlinger i e-tinglysnings-systemet. Bemærk, at de ”særlige handlinger” som en bruger med et certifikat registreret her vil kunne udføre afhænger af de brugerRoller certifikatet er tildelt.

Bemærk! Der gælder specielt at det certifikat, der udpeger en administrator, *ikke* kan anvendes ved anmeldelse af dokumenter til tinglysningsretten.

Selve Certifikat klassen indeholder en række attributter til at identificere certifikater i forbindelse med at e-tinglysnings-systemet checker, om et givet certifikat kan anvendes ved log-in og/eller ved underskrift af en anmeldelse. Disse attributter anvender engelske navne for at sikre konsistent brug i forhold til X.509 Certificate standarden.

- type – En type som angiver hvilket slags certifikat som er anvendt til identifikation. Dette kan generelt være POCES, MOCES eller VOCES selvom det i kontekst af brugerdata-basen typisk vil være MOCES og VOCES certifikater. I fremtiden vil der kunne åbnes op for andre typer af certifikater, f.eks. i forbindelse med udenlandske firmaers brug af e-tinglysnings.
- subject – Det fulde indhold af subject feltet i X.509 standarden
- subjectCommonName – CN elementet af subject feltet fra X.509 standarden.
- subjectSerialNumber – For danske OCES certifikater vil dette være PID:xxxx-xxxx-x-xxxxxxxxxxxxxx (POCES), CVR:xxxxxxxx-RID:xxxxxxxx (MOCES) og CVR:xxxxxxxx-UID:xxxxxxxx (VOCES). En fremtidig anvendelse af generelle X.509 certifikater vil specificere indholdet af subjectSerialNumber
- issuer – Det fulde indhold af issuer feltet fra X.509 standarden.
- issuerCommonName – Et udtræk af CN elementet fra issuer feltet.

Der vil blive defineret flere attributter for Certifikat klassen efterhånden som behovene af-dækkes.

5.4.3 Proces og Use-Cases

5.4.3.1 Oprettelse af registreret bruger

Anmodning om oprettelse indsendes på papir til Tinglysningsretten og forudsættes at være underskrevet af tegningsberettigede for virksomheden.

Ved oprettelsen angives certifikater for den/de administratorer, som på virksomhedens vegne har lov til at administrere yderligere certifikater for virksomheden.

For virksomheder med danske OCES certifikater angives administratorer ved:

- Indtastning af UID:xxxxxxxx for den eller de virksomhedscertifikater, der kan anvendes til administration

- Indtastning af RID: xxxxxxxx for den eller de medarbejdercertifikater, der kan anvendes til administration
- Upload af de konkrete MOCES eller VOCES certifikater, som kan anvendes til administration. Denne metode vil være den anbefalede måde at registrere certifikater på.

Ud over at tildele en eller flere administratorer ved oprettelsen, udpeger Tinglysningsretten de *bruger roller* som administratorerne vil kunne tildele til enkelte certifikater.

5.4.3.2 Vedligehold af administratorer

Tinglysningsretten kan til enhver tid gå ind og slette eksisterende eller tilføje nye administratorer på vegne af virksomheden, såfremt et certifikat er blevet væk eller en medarbejder, der har fungeret som administrator, har forladt virksomheden.

Den yderligere administration af information for en registreret bruger varetages af den eller de administratorer, som er udpeget i forbindelse med oprettelsen som registreret bruger.

Der implementeres *ikke* delegering af administratorrettigheder, da det må anses for yderst sjældent at virksomheder vil have brug for denne facilitet. Ønskes administratoren ændret, kan dette ske ved anmodning til Tinglysningsretten.

5.4.3.3 Administration af certifikater

Administratorer udpeget for virksomheden kan tilføje yderligere medarbejder- eller virksomheds-certifikater, samt tildele konkrete brugerroller til et certifikat blandt de brugerroller Tinglysningsretten har tilladt for den registrerede bruger (virksomheden).

Oprettelsen foregår efter samme princip som ved oprettelsen af certifikaterne for administratorerne, nemlig ved, at der angives UID: xxxxxx, RID: xxxx eller ved, at det konkrete X.509 certifikat uploades.

For hver anmelder kan administratoren afkrydse de bruger roller (blandt de tilladte) et givet certifikat giver ret til at benytte.

5.5 Storkundeordning

5.5.1 Indledning

Forbehold: Da reglerne vedrørende storkundeordningen er under genovervejelse, og SKAT ikke har mulighed for at specificere i hvilket omfang de ønsker at modtage informationer fra e-tinglysning tages der forbehold for beskrivelsen af storkundeordningen.

Professionelle brugere af tinglysningsystemet kan af SKAT tildeles status som storkunde.

Storkundestatus medfører at anmeldelser kan fremsendes til Tinglysningsretten uden at der afregnes tinglysningsafgift ved anmeldelsen. I stedet indbetaler storkunder afgifter direkte til SKAT.

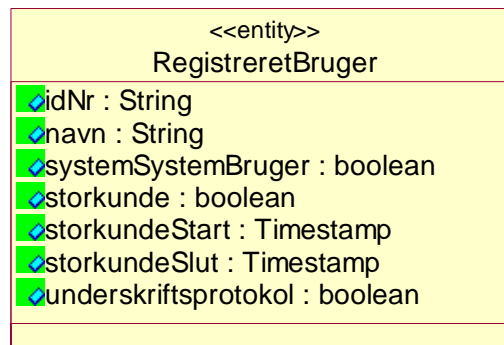
Til kontrol indberetter e-tinglysning information om de tinglysningstransaktioner, som er foretaget under storkundestatus.

Information om tildeling og/eller fratagelse af storkundestatus modtages i e-tinglysning via service-snitflade fra SKAT.

Informationen om hvorvidt en anmelder er tildelt storkundestatus opbevares på entiteten RegistreretBruger.

5.5.2 Model

5.5.2.1 UML



5.5.2.2 Beskrivelse

Klassen for RegistreretBruger indeholder attributter til indikation af den registrerede anmelders storkundestatus.

Attributten storkunde kan antage værdien true/false alt efter om den registrerede anmelder har storkundestatus. Attributterne storkundeStart og storkundeSlut indikerer tidspunkter for den registrerede anmelders oprettelse/nedlæggelse som storkunde.

Af- og tilmelding til storkundeordning registreres med historik.

5.5.3 Proces og Use-Cases

5.5.3.1 Ændring af storkundestatus

Tinglysningsretten modtager information omkring storkunder fra SKAT via en servicesnitflade. Det forventes at servicesnitfladen udgøres af en eller flere Webservice kald fra SKAT til e-tinglysning (push model).

Det er endnu ikke fastlagt, hvorvidt der modtages et kald per opdatering (CVR nummer), eller om der modtages information i batch, således at et antal tildelinger/fratagelser modtages samlet.

Udestående: Såvel servicesnitflade som det datamæssige indhold af informationer om tildeling og fratagelse af storkundestatus fra SKAT er ikke beskrevet.

Ved modtagelse af en *tildeling* af storkundestatus opdaterer e-tinglysning den Registreret-Bruger instans svarende til CVR nummeret således at `storkunde` sættes til `true`, `storkundeStart` til tidsstempel for transaktionen og `storkundeSlut` til `null`.

Ved modtagelse af en *fratagelse* af storkundestatus opdaterer e-tinglysning den Registreret-Anmelder instans svarende til CVR nummeret, således at `storkunde` sættes til `false` og `storkundeSlut` til tidsstempel for transaktionen.

5.5.3.2 Forespørgsel af storkundestatus

Forskellige delsystemer i e-tinglysning har behov for at kunne forespørge på storkundestatus for en registreret bruger.

Storkundestatus kan via servicekald oplyses på baggrund af CVR nummer.

5.6 System-system ordning

5.6.1 Indledning

System-system ordningen er den konkrete registrering i e-tinglysningsystemet vedrørende en virksomheds tilgang til systemet via system-system kommunikation.

Ordningen omfatter en registrering af, at virksomheden er godkendt som system-system bruger af Tinglysningsretten samt hvilket/hvilke certifikater, der kan anvendes til underskrift af system-systemkald foretaget af virksomheden.

De certifikater, der registreres som system-system certifikater under system-system ordningen, er de certifikater, som anvendes i forbindelse med WS-Security. Brugen af WS-Security i forbindelse med system-system kommunikation er beskrevet i afsnit 5.3.2.3 "System-system adgang".

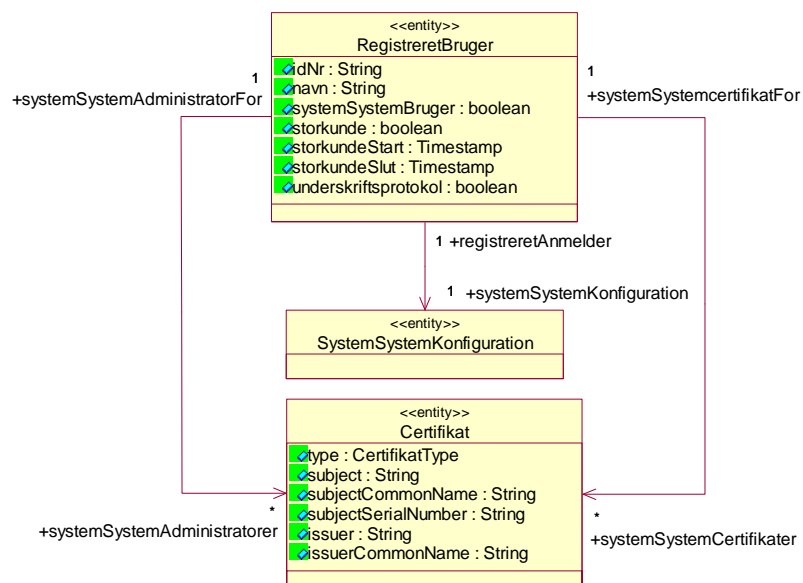
Ud over registreringen af system-system certifikaterne kan der registreres en eller flere certifikater for brugere, der kan administrere system-system ordningen på vegne af virksomheden. Denne registrering og anvendelse sker efter samme principper som for administratorer af brugerdatabase beskrevet i 5.4 "Brugerdatabase".

Administratorer af en system-system ordning vil kunne opsætte en række parametre, der konfigurerer virksomhedens tilgang til e-tinglysningsystemet, og hvordan systemet tilgår services hos virksomheden.

De konkrete parametre administratorerne kan vedligeholde er ikke fastlagt pt., men dele af de informationer, der kan konfigureres, vil blive opbevaret i e-tinglysning databasen, mens andre vil blive opbevaret i det *Service Registry (UDDI)*, der anvendes af e-tinglysningsystemet. De informationer, der vil blive opbevaret i Service Registry, vil omfatte adresser (end-points) på de services e-tinglysning vil kunne kalde hos virksomheden.

5.6.2 Model

5.6.2.1 UML



5.6.2.2 Beskrivelse

Som øvrige ordninger, er system-system ordningen bygget op omkring entiteten `RegistreretBruger`, som indeholder et flag (`systemSystemBruger`), der er sat til `true`, hvis den registrerede anmelder er godkendt som system-system bruger.

Bemærk! Af hensyn til afregning af tinglysningsafgifter, skal system-system brugere være registreret som storkunder hos SKAT.

Gennem relationen `systemSystemCertifikater` registreres de Certifikat entiteter, der repræsenterer X.509 certifikater som anvendes af virksomheden til underskrift af SOAP kald (WS-Security).

Relationen `systemSystemAfadministratorer` udpeger de certifikater som kan anvendes ved administration af system-system ordningen.

Konfigurationsparametre for den konkrete system-system ordning vil blive opbevaret i e-tinglysningsdatabasen, samt i det Service Registry der hører til løsningen. De konkrete registreringer i databasen repræsenteres af `SystemSystemKonfiguration` entiteten.

Bemærk: De specifikke konfigurationsparametre for system-system ordningen er ikke endeligt fastlagt, ligesom hvilke der placeres i databasen og hvilke som registreres i Service Registry ikke er endeligt afgjort.

5.6.3 Proces og Use-Cases

5.6.3.1 Opret system-system bruger

Aktør: Administrator i Tinglysningsretten

Administratoren fremsøger en registreret bruger eller opretter denne som beskrevet under brugerdata-basen. Der afkrydses at den registrerede bruger er godkendt som system-system bruger, og der indtastes information om den/de administratorer (certifikater), der kan anvendes til at administrere ordningen.

Ordningen vil først være aktiv, når en af administratorerne for virksomheden har været inde og opsatte de fornødne parametre.

5.6.3.2 Nedlæg system-system bruger

Aktør: Administrator i Tinglysningsretten

Administratoren fremsøger en registreret bruger og fjerner markeringen for, at denne er godkendt som system-system bruger. Dette vil ophæve system-system ordningen for virksomheden øjeblikkeligt og ikke længere tillade, at administratorer for virksomheden vedligeholder information om ordningen.

5.6.3.3 Vedligehold system-system parametre

Aktør: Virksomhedsadministrator for system-system ordning

Administratoren logger ind via den eksterne portal for at vedligeholde konfigurationsparametre for system-system ordningen.

Bemærk! Denne konfiguration kan kun foretages via den eksterne portal.

5.7 Anmelderordning

5.7.1 Indledning

Formålet med anmelderordningen er at muliggøre, at særligt autoriserede anmeldere kan underskrive anmeldelsesdokumenter på vegne af disponenten, uden at underskriften refererer til en fuldmagt i e-tinglysningssystemet. Anmelderen står dermed selv inde for at have den fornødne fuldmagt til at underskrive dokumentet på vegne af disponenten.

Anmelderordningen er begrænset til at omfatte *panterettigheder* (nye og påtegninger) og *ejendomsforbehold* (biler).

Enhver *registreret bruger* (se afsnit 5.4 ”Brugerdatabasen”) kan med Tinglysningsrettens godkendelse få oprettet en eller flere *anmelderordninger* som autoriserer en eller flere anmeldere (identificeret ved specifikke certifikater) fra virksomheden til at underskrive anmeldelser på vegne af en disponent (debitor).

De certifikater, som kan anvendes til underskrift under en anmelderordning, vil være en *delmængde* af de certifikater en registreret bruger har oprettet som værende berettiget til at underskrive anmeldelser. Det er en *administrator*, som på vegne af den registrerede anmelder konfigurerer hvilke certifikater, der kan anvendes under en given anmelderordning for den registrerede anmelder.

Tinglysningsretten opretter den konkrete anmelderordning og opretter i den forbindelse en eller flere administratorer, som kan foretage den videre administration af anmelderordningen. I denne proces opsætter Tinglysningsretten ligeledes et maksimalt beløb for de panterettigheder anmelderen kan indsende under anmelderordningen. Oprettelsen sker på baggrund af anmodning fremsendt til Tinglysningsretten på papir. Det forudsættes, at denne anmodning indeholder information om administrator(er), og at den er underskrevet af den eller de tegningsberettigede for virksomheden.

Tinglysningsretten kan til enhver tid tilbagekalde en eller flere af de anmelderordninger, der er oprettet for en registreret bruger.

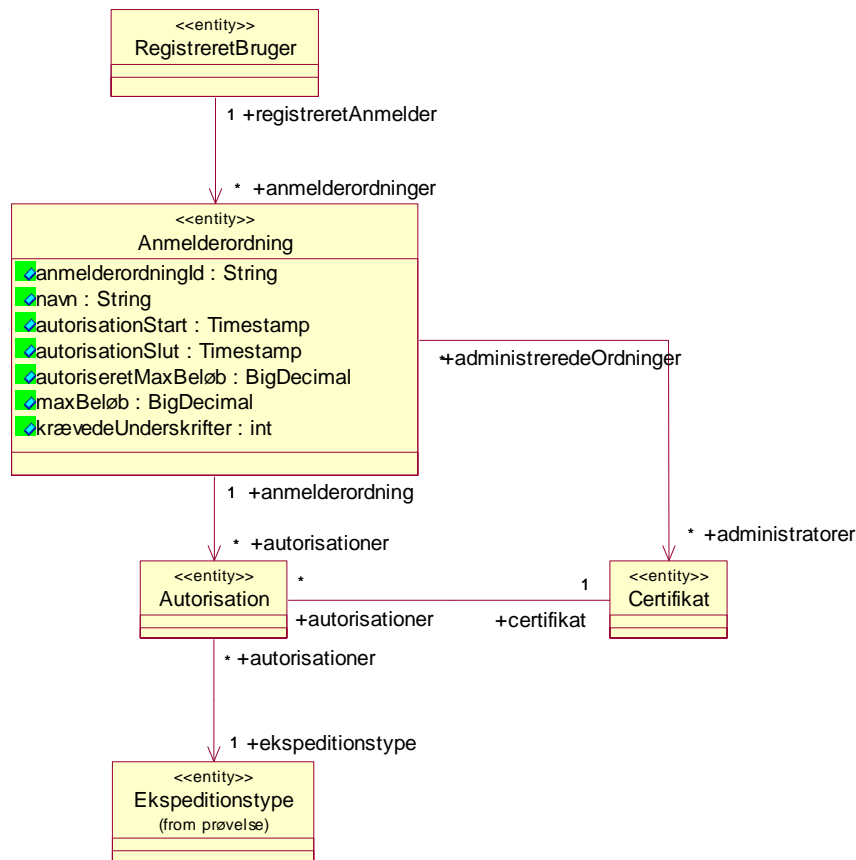
Administratorerne for anmelderordningen kan vedligeholde et maksimalt beløb for anmeldelsen af panterettigheder under en konkret anmelderordning. Dette beløb skal være mindre end eller lig med det maksimalt autoriserede beløb som Tinglysningsretten har specificeret. Ligeledes konfigurerer administratorerne hvor mange underskrifter, som kræves ved underskrift på vegne af en disponent.

De certifikater, der kan underskrive under en given anmelderordning, konfigureres af administratorerne, således at der for hvert certifikat opsættes regler (autorisation) for hvilke ekspeditionstyper det enkelte certifikat kan anvendes til at underskrive.

Eksempel: En administrator har konfigureret således at der kræves 2 underskrifter på vegne af en disponent. Under den registrerede anmelder er der 6 certifikater som kan anvendes til underskrift generelt. Administratoren vælger 3 certifikater og tillader at disse *kun* underskriver pantebreve i biler, mens de 3 resterende kan underskrive alle ekspeditionstyper under anmelderordningen.

5.7.2 Model

5.7.2.1 UML



5.7.2.2 Beskrivelse

Enhver Anmelderordning er associeret med en RegistreretBruger som udtryk for hvem autorisationen er tildelt, og tildeles derudover en unik identifikation i form af anmelderordningId. Identifikationen vil være unik på tværs af registrerede brugere.

Attributten navn er alene et navn, som kan anvendes til visuel genkendelse af anmelderordningen, og kan være navnet på den registrerede bruger, en afdelingsbetegnelse eller lignende.

Til begrænsning af pantet, som anmeldes under anmelderordningen, angives autoriseretMaxBeløb, og alt pant med værdi skarpt større end beløbet afvises under anmelderordningen.

En anmelderordning tidsstemples ved oprettelse, således at autorisationStart angiver fra hvilken dato anmelderordningen er *aktiv*. Attributten autorisationSlut efterlades tom (null) som udtryk for at anmelderordningen er *aktiv*. Ved inddragelse af autorisationen sættes autorisationSlut til et tidsstempel for ophøret af anmelderordningen, og anmelderordningen vil betragtes som *inaktiv* efter dette tidspunkt. En anmelderordning kan på et vilkårligt tidspunkt genaktiveres gennem den interne portal.

Ved oprettelsen udpeger Tinglysningsretten en eller flere administratorer (Certifikat). Dette sker på baggrund af den skriftlige anmodning tinglysningsretten har modtaget for virksomheden. Anmodningen forventes at være underskrevet af de en/flere tegningsberettigede for virksomheden.

Administratorer for en konkret anmelderordning vedligeholder felterne `maxBeløb` og `krævedeUnderskrifter`.

Attributten `maxBeløb` er den registrerede anmelders begrænsning af pantebeløb under anmelderordningen, og dette beløb skal være mindre end eller lig med `autoriseretMaxBeløb` angivet af Tinglysningsretten.

Antallet af krævede underskrifter (`krævedeUnderskrifter`) kan sættes til en værdi større end eller lig med 1.

Administratorer kan autorisere en eller flere certifikater til anvendelse i forbindelse med underskrift på vegne af disponenten. Dette sker ved at oprette et antal autorisationer (`Autorisation`), som sammenknytter `Anmelderordning`, `Certifikat` og `Ekspeditionstype`. Denne konstruktion i modellen tillader, at administratoren kan konfigurere hvilke certifikater, som kan anvendes i forbindelse med hvilke ekspeditionstyper.

Bemærk! Klassen `Autorisation` indeholder ikke egne attributter, men anvendes alene til sammenknytning af `Anmelderordning`, `Certifikat` og `Ekspeditionstype`. Konstruktionen tillader dog senere, at der indføres specielle flag eller attributter, som er specielle for den enkelte autorisation.

5.7.3 Proces og Use-Cases

5.7.3.1 Oprettelse

Tinglysningsretten fremsøger en *registreret bruger* via `idNr` (f.eks. CVR nummer), og vælger “opret autorisation”.

Systemet tildeler anmelderordningen en identifikation i form af `anmelderordningId`, knytter ordningen sammen med den registrerede anmelder og foreslår `autoriseretStart` tidspunktet.

Tinglysningsretten udfylder navn og tildeler en eller flere administratorer til anmelderordningen. Administratorer udvælges blandt certifikater fra den registrerede anmelder.

Slutteligt udfylder tinglysningsretten det maksimale beløb for pant anmeldt under anmelderordningen (`autoriseretMaxBeløb`).

5.7.3.2 Nedlæggelse

Tinglysningsretten fremfinder en *registreret bruger* via `idNr` (f.eks. CVR nummer). Fra detaljesiden for den registrerede anmelder kan *listen* af anmelderordninger for den registrerede anmelder tilgås.

Fra listen vælges en eller flere autorisationer og der vælges “inddrag autorisation”.

Systemet nedlægger de valgte anmelderordninger og foreslår `autorisationSlut` feltet til det aktuelle tidspunkt.

5.7.3.3 Vedligehold af administratorer

Tinglysningsretten kan på et vilkårligt tidspunkt tilføje eller fjerne administratorer for hver af de anmelderordninger oprettet for en registreret bruger.

5.7.3.4 Konfiguration af anmelderordning

Administratorer kan vedligeholde information som navn, `maxBeløb` og `krævedeUnderskrifter` for de anmelderordninger de er administratorer for.

5.7.3.5 Konfiguration af autorisationer

Ved oprettelse af autorisationer udvælger en administrator et certifikat blandt de certifikater, som er oprettet for den registrerede bruger. Herefter vises en liste af ekspeditionstyper, der kan anvendes, og de som administratoren ønsker at certifikatet skal have lov til at anvende afkrydses.

Hvis administratoren senere ønsker at omkonfigurere autorisationerne, fremkaldes det certifikat, som ønskes omkonfigureret, og afkrydsningen af ekspeditionstyper ændres.

En administrator kan på et vilkårligt tidspunkt udvælge et certifikat og fjerne det fra anmelderordningen. Herved fjernes alle autorisationer, som er knyttet til certifikatet for den konkrete anmelderordning.

Bemærk! Hvis et certifikat fjernes fra listen af certifikater under den registrerede anmelder vil alle tilhørende autorisationer for alle anmelderordninger under den registrerede anmelder blive slettet.

5.8 Underskriftsdatabasen

5.8.1 Indledning

Underskriftsdatabasen benyttes i forbindelse med anmeldelser, hvor en virksomhed optræder som *disponent*.

Generelt kan virksomheder kun disponere gennem underskrifter fra de *tegningsberettigede*, i henhold til virksomhedens *tegningsregler*, som registreret hos Erhvervs- og Selskabsstyrelsen.

For en særlig gruppe af virksomheder kan dispositionsretten videregives til en eller flere af virksomhedens medarbejdere. Denne særlige gruppe af virksomheder omfatter:

... virksomheder hvis formål er at foretage belåning og salg af den type aktiviteter, der er registreret hos Tinglysningsretten ...

Virksomheder, der tilhører denne særlige kategori, kan få registreret medarbejdere med prokura til at disponere på virksomhedens vegne indenfor konkrete afgrænsede ekspeditioner. Disse registreringer opbevares i e-tinglysningsystemets *underskriftsdatabase*.

Vi forventer at der fra Erhvervs- og Selskabsstyrelsen stilles en service til rådighed, der tillader at tegningsregler for en virksomhed checkes via online opslag. Indtil denne funktionalitet er tilgængelig vil dette check skulle gennemføres ved manuel behandling.

Ved modtagelse af en anmeldelse, hvor en virksomhed optræder som disponent, checkes det først om virksomheden er registreret hos Tinglysningsretten som hørende til den særlige gruppe af virksomheder hvis formål er at foretage belåning og salg af den type aktiviteter, der behandles hos Tinglysningsretten. Hvis dette er tilfældet checkes underskrifterne mod *underskriftsdatabasen*.

I modsat fald checkes underskrifterne mod E&S (CVR), for at fastslå hvorvidt underskrifterne er korrekte i forhold til tegningsreglerne for virksomheden.

I *underskriftsdatabasen* registreres således de medarbejdere, der ikke tilhører kredsen af tegningsberettigede, men som har fået prokura til at disponere på virksomhedens vegne.

Eksempel: En bank ønsker at give prokura til en række medarbejdere i forbindelse med aflysning af pantebreve. Reglen kan være at for pantebreve op til 10.000.000,- kræves underskrift af 2 af bankens medarbejdere med særlig prokura til aflysning af pantebreve. For pantebreve over 10.000.000,- kræves underskrift af en af medarbejderne i forening med en af cheferne i pantebrevsafdelingen.

Dette kan realiseres ved at virksomheden registrerer en række *tegningsregler*, der ud over at indeholde regler om rolle, maksimalt beløb og ekspeditionstyper også refererer til medarbejdere placeret i et antal *tegningsgrupper*. Tegningsgrupper i forening men tegningsregler kan – men behøver ikke – opfattes som en slags *stillingsprokura*.

De tegningsregler som udtrykkes i ovenstående eksempel, kan systemmæssigt repræsenteres som det er skitseret i figur 2 og figur 3 nedenfor.

Tegningsregel: Aflysning af pantebreve
Rolle: KREDITOR
Maksimalt beløb: 10.000.000,-
Ekspeditionstyper: AflysningHæftelseFastEjendom

Tegningsgruppe: Pantebrevsafdelingen
Antal underskrifter: 2
(Refererer til 10 certifikater for medarbejdere i pantebrevsafdelingen)

Figur 2: Tegningsregel for aflysning af pantebreve under 10.000.000,-

Tegningsregel: Aflysning af pantebreve (> 10.000.000,-)

Rolle: KREDITOR

Maksimalt beløb: -

Ekspeditionstyper: AflysningHæftelseFastEjendom

Tegningsgruppe: Pantebrevsafdelingen

Antal underskrifter: 1

(Refererer til 10 certifikater for medarbejdere i pantebrevsafdelingen)

Tegningsgruppe: Chefer for kreditgivning

Antal underskrifter: 1

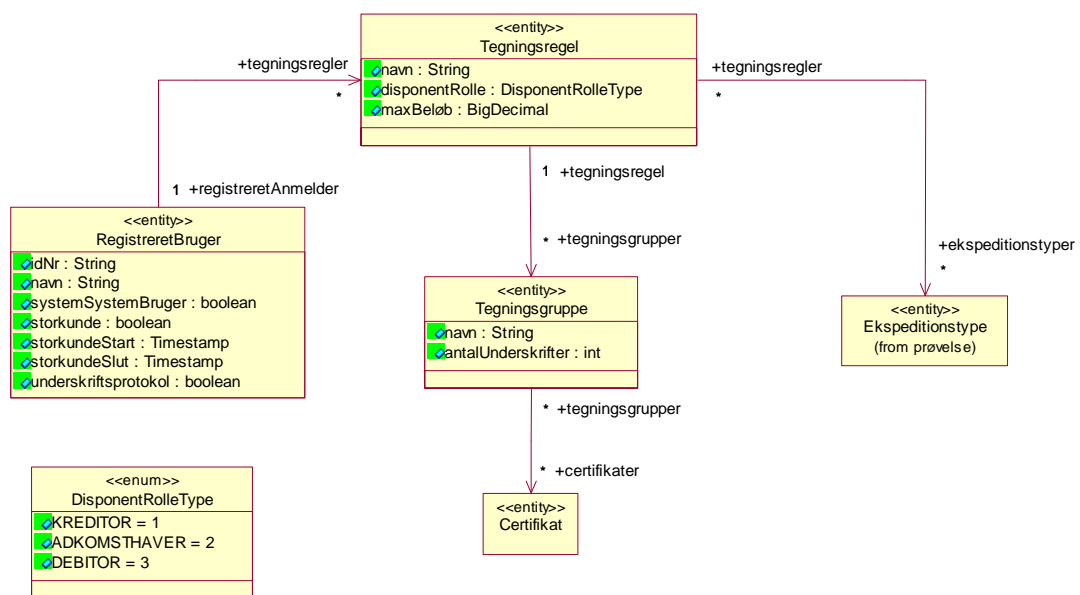
(Refererer til 4 certifikater tilhørende chefer i kredit selskabet)

Figur 3: Tegningsregel for aflysning af pantebreve over 10.000.000,-

Bemærk at indenfor en tegningsregel sættes der *OG* mellem underskrifter fra de enkelte tegningsgrupper, således skal der i figur 3 indhentes underskrift fra 1 medarbejder i gruppen “Pantebrevsafdelingen” *OG* 1 medarbejder i gruppen “Chefer for kreditgivning”.

5.8.2 Model

5.8.2.1 UML



5.8.2.2 Beskrivelse

Modellen afspejler at de tegningsregler (Tegningsregel) som opbevares i e-tinglysningsystemet er knyttet op på en RegistreretBruger entitet.

Hver tegningsregel kan udpege et antal ekspeditionstyper som den enkelte tegningsregel dækker, sammen med en samling af tegningsgrupper. Tegningsgrupperne udgør en måde at gruppere et antal konkrete certifikater på.

5.8.3 Proces og Use-Cases

5.8.3.1 Registrering af virksomhed

Modellen antager at Tinglysningsretten vurderer og vedligeholder informationen om hvorvidt en virksomhed er i gruppen af virksomheder "... hvis formål er belåning og salg...". Dette sker ved at fremsøge den registrerede bruger og opdatere feltet underskriftsprotokol (afkrydsningsfelt).

Hvis der sker ændring af virksomhedens formål, startes en workflow opgave, som muliggør, at Tinglysningsretten kan revurdere om virksomheden har lov til at anvende funktionaliteten i underskriftsdatabase.

Efter afkrydsning af feltet vil administratorer fra den registrerede anmelder kunne vedligeholde tegningsregler, tegningsgrupper og certifikater som indgår i tegningsgrupperne.

5.8.3.2 Vedligehold af tegningsregler

De administratorer, der er udpeget for den registrerede bruger, kan – hvis Tinglysningsretten har åbnet for muligheden – kunne administrere tegningsregler, tegningsgrupper og certifikater som indgår i tegningsgrupperne.

Bemærk! Hvis et certifikat fjernes fra den registrerede bruger, vil det ikke længere optræde som en del af de tegningsgrupper, det tidligere har indgået i.

Adgangen (system-system kald eller via den eksterne portal) vil give *en bruger* mulighed for at

- få vist samtlige registrerede underskriftsberettigede for en given virksomhed
- for hver underskriftsberettiget angivelse af hvilken rolle den pågældende har
- for hver underskriftsberettiget angivelse af hvilke ekspeditionstyper, der må benyttes
- maxBeløb for ekspeditionstypen
- evt. antal nødvendige signaturer anvendt sammen med den konkret viste signatur

En bruger med administrator-rettigheder skal:

- kunne tilføje nye medarbejdersignaturer for den virksomhedssignatur, administratoren tilhører
- kunne angive/ændre rettigheder for medarbejdersignaturer: vedr. roller, ekspeditionstyper mv.
- kunne slette signaturer fra Underskriftsdatabase.

5.8.3.3 Kontrol af tegningsregler

Betydningen af tegningsregler er at sikre, at den forkerte person ikke kan disponere på vegne af en virksomhed, selskab, forening etc.

Prøvelsen af dispositionsretten gælder for alle anmeldelser. Ved autoriserede anmeldere samt ved fuldmagtsordningen træder særregler imidlertid ind for disponenten. Jf. beskrivelsen af disse ordninger.

Men alle ekspeditionstyper (som ikke sker gennem ovennævnte anmelder- eller fuldmagtsordning) skal - i tilfælde af at den er signeret af anden type disponent end CPR (dvs. med andet end POCES certifikat) - gennemgå kontrollen KontrolTegningsret. Denne skal, såfremt disponenten ikke har CPR, men underskriver med digital signatur, sørge for at dirigere anmeldelsesdokumentet til manuel behandling. Dette sker *kun* hvis der i MOCES certifikatet ikke er angivet et CPR nummer.

5.9 Fuldmagtsordningen

5.9.1 Indledning

Fuldmagtsordningen introduceres for at tillade de personer/virksomheder, der ikke har mulighed for – eller ønske om – at foretage digital anmeldelse/underskrift, at kunne give fuldmagt til tredjepart, som f.eks. professionelle rådgivere, for så vidt angår underskriften.

En fuldmagt kan således indsendes til Tinglysningsretten på papirblanket, hvor den registreres i e-tinglysningssystemet via den interne portal. Selvom fuldmagtsordningen primære formål er at understøtte personer/virksomheder *uden* digital signatur, vil fuldmagter kunne registreres af *fuldmagtsgiver* på den eksterne portal.

Ved anvendelse af en registreret fuldmagt vil *fuldmagtshaverens* underskrift dermed stå i stedet for *fuldmagtsgiverens*.

Indholdet af en fuldmagt som registreres hos Tinglysningsretten omfatter:

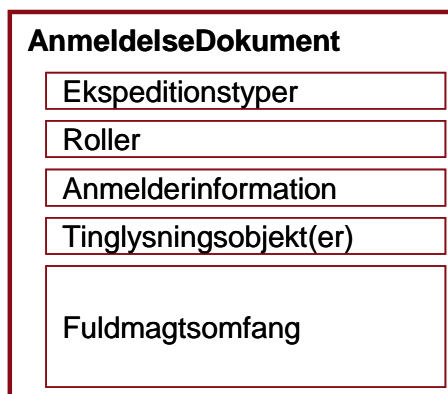
- **Fuldmagtstype** – den overordnede type af fuldmagten, der angiver hvilken overordnet anvendelse fuldmagten har (fast ejendom, pantsætning af bil, etc.). Denne type sætter begrænsning for de *tinglysningsobjekter*, *dispositioner* og *erklæringer* fuldmagten kan indeholde, jf. beskrivelse af disse nedenfor.
- **Anmelder** – den som anmelder fuldmagten til tinglysningsretten identificeret ved den tinglysningsmæssige *rolle* med angivelsen af CPR/CVR, navn, adresse, telefon og e-mail adresse, samt evt. de yderligere informationer der kan indeholdes i en anmeldelse vedrørende anmelderen (kontaktperson, sagsnummer etc.)
- **Fuldmagtsgiver** – den som giver sin fuldmagt til at lade fuldmagtshaveren disponere på sine vegne. Er identificeret som fuld tinglysningsmæssig *rolle*, med CPR/CVR, navn, adresse, telefon og e-mail adresse.
- **Fuldmagtshaver** – den som får fuldmagt til at foretage digital anmeldelse/underskrift på vegne af fuldmagtsgiveren. Er identificeret som en fuld tinglysningsmæssig *rolle* med angivelse af CPR/CVR nummer, navn, adresse, telefon og e-mail adresse.
- **Tinglysningsobjekt(er)** – referencer til de tinglysningsmæssige objekter fuldmagten omfatter, dvs. ejendomme, biler, personer, virksomheder, andelsboliger eller eksisterende tinglyste dokumenter (påtegning). Tinglysningsobjekterne afhænger af ekspeditionstypen, samt fuldmagtstypen.
- **Rolle(r)** – den/de roller som *fuldmagtshaveren* kan antage på vegne af *fuldmagtsgiveren*.
- **Disposition(er)** – angivelse af de dispositioner *fuldmagtshaveren* kan foretage på vegne af *fuldmagtsgiver* identificeret ved et antal *ekspeditionstyper* der angives i fuldmagten.
- **Erklæring(er)** – angivelsen af en eller flere *erklæringer* som fuldmagtshaveren kan afgive på vegne af fuldmagtsgiveren. Erklæringskoder kan evt. være samlet i grupper, således at der let kan angives en række erklæringer ved et valg.
- **Beløbsgrænse** – en krævet beløbsgrænse for *fuldmagtshaverens* ret til at disponere.
- **Gyldighedsperiode** – en krævet gyldighedsperiode for fuldmagtens gyldighed i form af en fra og til dato.
- **Videreoverdragelse** – angivelse af hvorvidt *fuldmagtshaveren* har ret til at videreoverdrage fuldmagten.

5.9.2 Model

5.9.2.1 AnmeldelseDokument

Strukturen af anmeldelsesdokumentet for indsendelse af en fuldmagt følger den overordnede struktur beskrevet i dette afsnit.

Strukturen for den generelle de af anmeldelsesdokumenter er skitseret i figuren "AnmeldelseDokument for fuldmagt" nedenfor.

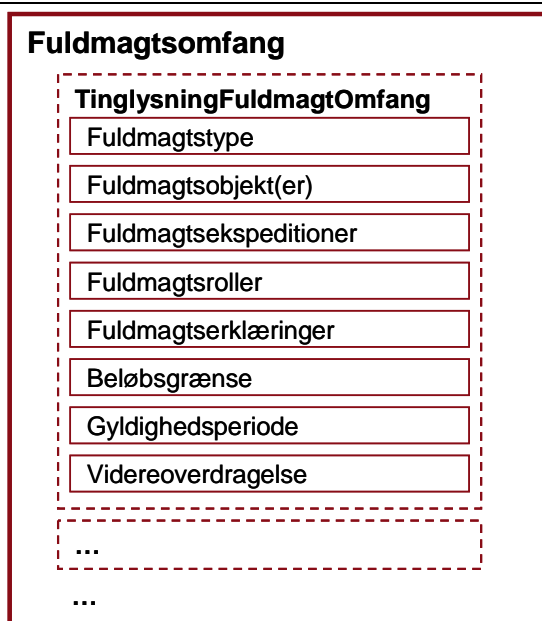


Figur 4: AnmeldelseDokument for fuldmagt

De enkelte sektioner indeholder følgende information:

- **Ekspeditionstyper** – der angives ekspeditionstypen for "NyFuldmagt" eller "TilbagekaldelseFuldmagt"
- **Roller** – Listen af de roller som indgår i fuldmagten angives på sædvanlig vis i anmeldelsesdokumentet med angivelsen af rolletype, CPR/CVR nummer, navn, adresse, telefon og e-mail.
De rolletyper som kan angives for fuldmagter omfatter "Anmelder", "Fuldmagtsgiver", "Fuldmagtshaver" og "Vitterlighedsvidne". Vitterlighedsvidner angives og registreres kun i det omfang fuldmagten fremsendes på papirblanket til Tinglysningsretten.
- **Anmelderinformation** – Den sædvanlige sektion i anmeldelsesdokumentet, der indeholder yderligere information om anmelderen.
- **Tinglysningsobjekter** – Generelt angives i anmeldelser her de tinglysningsmæssige objekter, der er en del af anmeldelsen. Man kunne således tro, at der her angives de objekter fuldmagten omfatter. I stedet er det dog referencer til *fuldmagtsgiver* og *fuldmagtshaver* i form af person/virksomhedsreferencer, der angives.
Selvom en fuldmagt er en registrering og ikke en *tinglysnings* sammenknyttes fuldmagtsgiver og fuldmagtshaver på samme måde som det kendes fra f.eks. en ægtepagt.
- **Fuldmagtsomfang** – Her placeres de informationer, der er specielle for registreringen af en fuldmagt. Se detaljerne for indholdet af denne sektion i Figur 5 nedenfor.
- **Bilag** – Generelt tillades ikke vedhæftning af bilag til anmeldelsen af fuldmagter, men når Tinglysningsrettens medarbejdere registrerer en fuldmagt modtaget på papirblanket, vedhæftes den indskannede fuldmagtsblanket som bilag.

Strukturen af sektionen "Fuldmagtsomfang", der indgår i anmeldelsesdokumentet ved anmeldelse af fuldmagter er skitseret i figur 5 nedenfor.



Figur 5: Struktur af sektionen "Fuldmagtsomfang"

De enkelte undersektioner i strukturen udgør den information, der fastlægger omfanget af den anmeldte fuldmagt.

- **Fuldmagtstype** – Angiver den overordnede fuldmagtstype. Fuldmagtstypen sætter de overordnede rammer for hvilke *fuldmagtsobjekt(er)*, *fuldmagtsekspeditioner*, *fuldmagtsrolle(r)* og *fuldmagtserklæringer* fuldmagten kan indeholde.
- **Fuldmagtsobjekter** – Specificerer den/de objekter fuldmagten omfatter, dvs. ejendomme, andelsboliger, personer, virksomheder, biler eller dokumenter (påtegning). Referencer til disse objekter angives på samme måde som der generelt angives referencer til *tinglysningsobjekter* i en anmeldelse.
- **Fuldmagtsekspeditioner** – En liste af ekspeditionstyper, der angiver hvilke ekspeditionstyper fuldmagten giver fuldmagtshaver ret til at underskrive på vegne af fuldmagtshaver. Referencer til disse ekspeditionstyper angives på samme måde som når der refereres til ekspeditionstyper i en anmeldelse.
- **Fuldmagtsroller** – En liste af rolletyper som specificerer hvilke roller fuldmagtshaver kan indtage på vegne af fuldmagtsgiver.
- **Fuldmagtserklæringer** – Her angives en liste af referencer til erklæringer fuldmagtshaver kan afgive på vegne af fuldmagtsgiver. Dette er altså ikke konkrete erklæringer som afgives men listen af de erklæringer som *kan* afgives.
- **Beløbsgrænse** – Det maksimale beløb fuldmagten omfatter ret til at disponere for i forbindelse med salg, pantsætning etc.
- **Gyldighedsperiode** – Den periode fuldmagten er gyldig angivet ved en fra dato og en til dato. Fuldmagtshaveren kan udelukkende anvende fuldmagten til dispositioner indenfor dette tidsinterval. Der er pt. ikke specificeret noget øvre grænse for hvor længe en fuldmagt kan gælde, men denne fastsættes formodentlig til ca. 6 måneder.
- **Videreoverdragelse** – Angivelse af hvorvidt fuldmagtshaver kan videreoverdrage fuldmagten til anden fuldmagtshaver.

Ved elektronisk anmeldelse af en ny fuldmagt angives ekspeditionstypen, roller (anmelder, fuldmagtsgiver og fuldmagtshaver), sædvanlig anmelderinformation, referencer til fuldmagtsgiver og fuldmagtshaver, samt den samlede information der kan indeholdes i sektionen fuldmagtsomfang.

Det er ved elektronisk anmeldelse ikke tilladt at vedhæfte bilag, som indgår i prøvelsen (der kan ikke registreres særlige individuelle betingelser for en fuldmagt).

Ved indsendelse af fuldmagt på papirblanket registreres anmeldelsen af Tinglysningsrettens medarbejder og den originale papirblanket indskannes og vedhæftes som bilag.

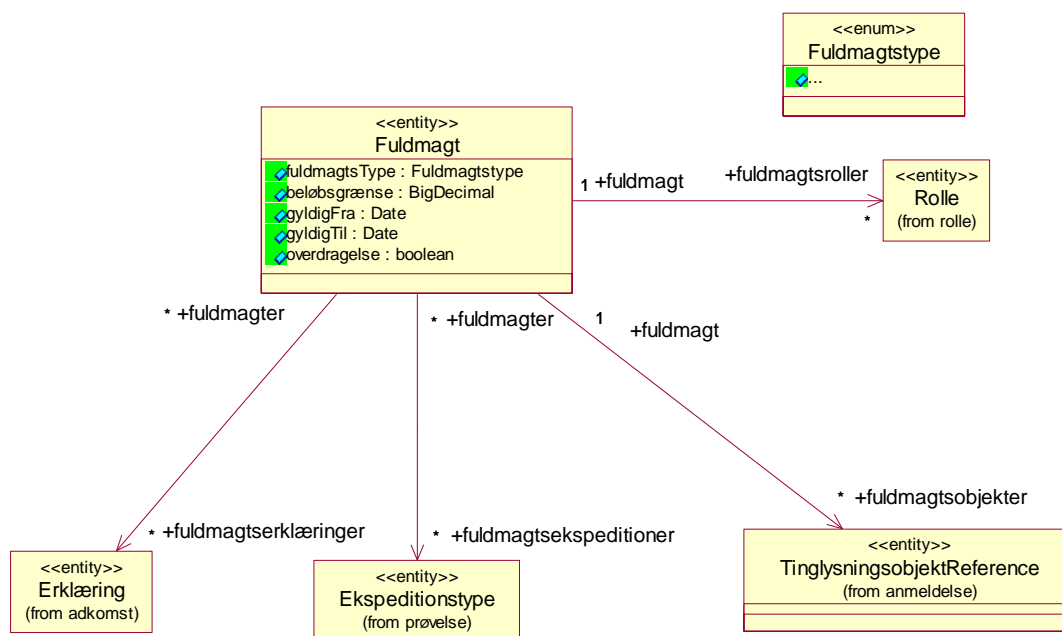
5.9.2.2 Generelle fuldmagter

Modellen for fuldmagter i e-tinglysning åbner op for at der på sigt defineres andre fuldmagtstyper end de som dækker tinglysningsområdet. Dette kunne være registreringer af fuldmagter som dækker ekspeditioner hos andre myndigheder.

Ved introduktion af en anden fuldmagtstype end den som anvendes i forbindelse med tinglysning benyttes den samme grundstruktur i anmeldelsesdokumentet (beskrevet i 5.9.2.1 ”AnmeldelseDokument”), mens der defineres et nyt konkret skema for indholdet af Fuldmagtsomfang elementet. Herefter vil Fuldmagtsomfang elementet skemamæssigt med en choice konstruktion kunne repræsentere *enten* en fuldmagt for tinglysningsområdet *eller* en fuldmagt for det nye område (osv.).

Der er ikke pt. konkrete planer for udvidelsen af fuldmagtsregistreringen hos Tinglysningsretten, men designet af anmeldelsen for fuldmagter tillader en udvidelse i fremtiden.

5.9.2.3 UML



5.9.3 Proces og Use-Cases

5.9.3.1 Anmeldelse af fuldmagt (ekstern portal)

Aktør: Anmelder (fuldmagtsgiver)

Anmelderen (fuldmagtsgiver) udsteder fuldmagt ved at udfylde anmeldelse på den eksterne portal på samme måde som andre anmeldelser til Tinglysningsretten.

Anmeldelsen af fuldmagten prøves automatisk, og vil efter godkendelse fremgå af ”Mine fuldmagter” for henholdsvis fuldmagtsgiver og fuldmagtshaver.

5.9.3.2 Anmeldelse af fuldmagt (system-system)

Fuldmagter som anmeldes via system-system kald indsendes som alle andre typer af anmeldelser, og underskrives af afsenderen som *anmelder* og evt. *fuldmagtsgiver*.

Hvis en system-system partner ønsker at indsende en fuldmagt på vegne af en anden *fuldmagtsgiver* skal vedkommende være opmærksom på at dennes underskrift indhentes på Tinglysningsrettens eksterne portal.

For yderligere information om underskrifter på den eksterne portal henvises til kapitel 4 ”Systemgrænseflader” i løsningsbeskrivelsen.

5.9.3.3 Anmeldelse af fuldmagt (blanket baseret)

Aktør: Medarbejder i Tinglysningsretten

Medarbejderen indscanner fuldmagtsblanketten og opretter fuldmagt i systemet baseret på de informationer som findes i fuldmagtsblanketten. Inddateringen af fuldmagten opsættes automatisk på baggrund af de OCR læste data. Medarbejderen foretager *manuel* prøvelse af underskrifterne på fuldmagten, herunder underskrifter fra *vitterlighedsvidner*.

Den indscannede blanket vedhæftes som bilag til fuldmagten.

Herefter fremgår fuldmagten i ”Mine fuldmagter” for henholdsvis fuldmagtsgiver og fuldmagtshaver.

5.9.3.4 Tilbagekaldelse af fuldmagt

Aktør: Fuldmagtsgiver

Fuldmagtsgiver kan via den eksterne portal (Mine fuldmagter) på ethvert tidspunkt tilbagekalde en udstedt fuldmagt. Herefter vil fuldmagten ikke kunne anvendes til dispositioner i forbindelse med tinglysning.

En fuldmagtsgiver vil kunne tilbagekalde en udstedt fuldmagt ved at indsende tilbagekaldelse på papirblanket til Tinglysningsretten. En medarbejder i Tinglysningsretten vil herefter registrere tilbagekaldelsen.

Hvis en fuldmagt indsendes via system-system kald returneres unik reference, der kan inkluderes i senere anmeldelser som reference til den konkrete fuldmagt. Ved anmeldelse af en fuldmagt via portalen returneres ligeledes den dannede unikke reference.

5.9.3.5 Kontrol af fuldmagt

Aktør: e-tinglysning motor

Kontrol af fuldmagter foretages i `KontrolFuldmagtsordning`.

5.9.3.6 Anvendelse af fuldmagt

Aktør: Anmelder (fuldmagtshaver)

Ved anmeldelse kan en anmelder angive, at en af de krævede underskrifter på anmeldelsen opfyldes af en allerede registreret fuldmagt, eller ved en forventet fuldmagt.

Konkret angives dette i tinglysningsdokumentet gennem elementet `AnvendtFuldmagt`, som kan indeholde reference til en tidligere anmeldt fuldmagt, eller specifikationen af en forventet fuldmagt. For yderligere information om strukturen af anmeldelsen i forhold til fuldmagter – og underskrifter i al almindelighed – henvises til løsningsspecifikationens kapitel 4 afsnit 4.2.5.2.

5.10 Anmeldte/tinglyste fuldmagter

5.10.1 Indledning

Fra tinglysningen af hæftelser og adkomstdokumenter kendes princippet om, at der afgives erklæringer, der reelt giver en af parterne fuldmagt til – evt. i begrænset omfang – at råde over den rettinghed, som anmeldelsesdokumentet er bærer af.

Et eksempel på en sådan “implicit” fuldmagt kunne være:

Meddelelser i henhold til retsplejelovens kapitel 51 og øvrige meddelelser, der efter loven skal sendes til pantekreditor, bedes sendt til

Pantekreditor, adresse, postnr. og by

der i øvrigt bemyndiges til på mine/vore vegne at underskrive påtegninger af enhver art på dette ejerpantebrev, herunder kvitterings-, transport-, moderations- og relationspåtegninger.

I et automatiseret tinglysningssystem bliver vi nødt til at kunne repræsentere den fuldmagtsmæssige konsekvens af sådanne erklæringer, således at når der modtages påtegninger, vil systemet automatisk kunne validere, at anmelderen (pantekreditor) faktisk er bemyndiget til at kunne skrive under på de nævnte påtegningstyper.

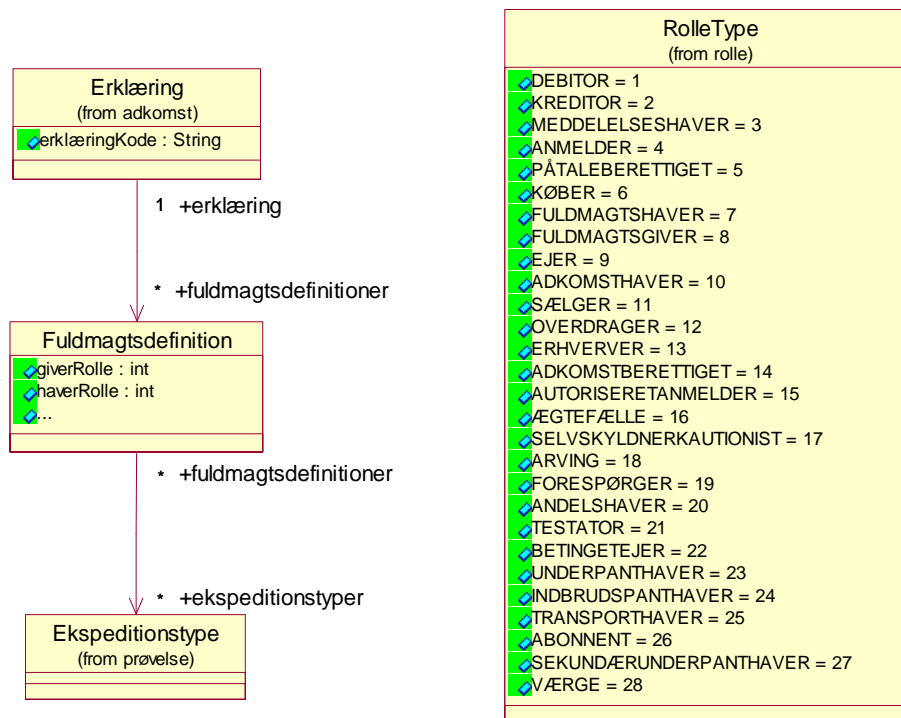
I e-tinglysningssystemet implementeres dette ved at erklæringer i Tinglysningsrettens erklæringskatalog kan tilknyttes en fuldmagtsdefinition, der på kodet form kan udtrykke sådanne “implicitte” fuldmagter.

Der angives ved anmeldelse at underskriften er tilstede via implicit fuldmagt.

Fuldmagtsdefinitioner knyttet til erklæringstekster i erklæringskataloget vedligeholdes af medarbejdere i Tinglysningsretten.

5.10.2 Model

5.10.2.1 UML



5.10.2.2 Beskrivelse

Hver Erklæring entitet kan referere til en eller flere Fuldmagsdefinition entiteter. Hver af disse entiteter beskriver i kodet form den ”implicitte” fuldmagt erklæringsteksten dækker over.

Fuldmagsdefinition entiteten indeholder information om fuldmagtsgiver- og fuldmagtshaverrollen (f.eks. debitor og kreditor), samt refererer til de ekspeditionstyper fuldmagten omfatter.

På Fuldmagsdefinition entiteten kan registreres yderligere begrænsninger i fuldmagtsomfanget, såfremt dette er nødvendigt.

Tinglysningsretten indeholder gennem den interne portal erklæringstekster, samt de fuldmagsdefinitioner disse tekster dækker over.

5.10.3 Proces og Use-Cases

5.10.3.1 Vedligehold af Fuldmagsdefinitioner

Aktør: Medarbejder i Tinglysningsretten

Medarbejderen i Tinglysningsretten opretter en eller flere fuldmagsdefinitioner for hver erklæringstekst, som kan give anledning til en anmeldt/tinglyst fuldmagt.

Dette sker på den interne portal.

5.10.3.2 Registrering af anmeldte/tinglyste fuldmagter

Aktør: e-TL motoren

Når en anmeldelse, som inkluderer erklæringstekster med implicite fuldmagter, modtages i e-tinglysningsmotoren, registreres disse som en del af berigelsen.

5.10.3.3 Kontrol af anmeldte/tinglyste fuldmagter

Aktør: Kontroller

Kontrollen af anmeldte/tinglyste fuldmagter sker i kontrollerne `KontrolTinglystFuldmagt`, `KontrolTinglystFuldmagtOmfang`, `KontrolTinglystFuldmagtSignatur`, `KontrolAnmeldtFuldmagt`, `KontrolAnmeldtFuldmagtOmfang`.

5.11 Afgiftsberegning

5.11.1.1 Beregnings Web Services

Den funktionalitet, som e-TL motoren indeholder til beregning af tinglysningsafgift, stilles til rådighed for de eksterne interessenter, som er system-system brugere og via portalen. Disse kan via webservice kald udføre to forskellige typer af afgiftsberegninger:

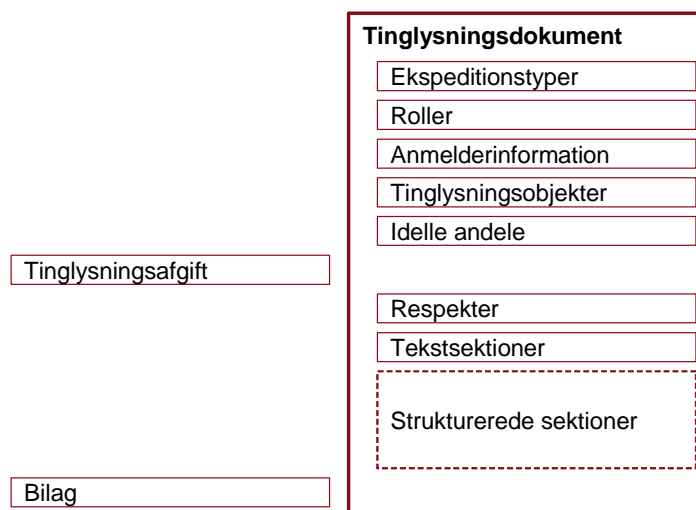
- Beregn samlet afgift
- Beregn variabel afgift ifbm. ny hæftelse/afløsningslån - med overført afgift fra eksisterende hæftelse(r)¹

Fælles for de to services gælder, at ekspeditionstypen altid skal fremgå af XML-dokumentet til 'afgiftsberegning'.

Således vil en bank eller et realkreditinstitut ved lånerådgivning/tilbudsgivning - kunne anvende e-TL's webservices direkte fra deres eget sagsbehandlingssystem. Ydelsen fra e-TL er gratis.

5.11.1.2 Proces

En system-system bruger udfærdiger en anmeldelse med sædvanlige data for denne - men eksklusiv tinglysningsafgift/afgiftsbeløb og eventuelle bilag:



Dette *anmeldelsesdokument* sendes som parameter til et servicekald Beregn afgift.

Ud fra ekspeditionstype samt dataindhold (afgiftspligtigt beløb) beregner KontrolAfgift og tilhørende kontroller den beregnede afgift.

XML-strukturen vil efter behandling i motoren blive "beriget" med strukturen for tinglysningsafgift. Det fulde tinglysningsdokument vil derefter blive returneret til system-system brugeren, som kan anvende XML'en videre i sit sagsbehandlingssystem. Alternativt gå direkte til anmeldelse overfor e-TL.

Således kan en kunde sikre sig på forhånd, at tinglysningsafgiften er korrekt angivet/beregnet, hvorved det undgås at anmeldelsen eventuelt udtages til afgiftskontrol.

¹ Kunden skal i servicekaldet inkludere dataløbenummer for alle hæftelser, der "ønskes" overført afgift fra. E-TL vil checke at disse eksisterer på kaldstidspunktet. Hvis de ikke gør, sendes en advarselstekst som del af afgiftssvaret til system-system-brugeren, men hæftelserne indgår "ukritisk" som afløsningslån i afgiftsberegningen.

Kun i helt specielle situationer, hvor der sker ændringer i afgiftssatserne, vil faktisk afgift ved tinglysningen kunne variere i forhold til den forhåndsberegnete.

Hvis der ønskes udført afgiftsberegning for et afløsningslån, skal der i anmeldelsesdokumentet medsendes et afgiftsgrundlag samt udpeges de hæftelser, som der ønskes overført afgift fra (når den rigtige tinglysning finder sted).

Det bemærkes at angivelse af dato + løbenummer ikke vil være nogen garanti for afgiftsberegningen, da det tidligere lån kan blive afløst før indsendelsen af det nye.

Det er krævet, for bestemte typer pantebrev (henvisning: Bilag 2 B, s. 181-182, KontrolAfløsningspantebrev) at bestemte erklæringer afgives ifm. oplysningerne om det nye lån.

For ekspeditionstyperne PantebrevFastEjendom(7), ForhøjelseFastEjendom(84) og UdvidelseHæftelseFastEjendom(88) kan anmelder således inkludere erklæring vedrørende:

"At långivningen sker på realkreditlignende vilkår og at

løbetiden på det nye lån minimum er 10 år, at regne fra tinglysningstidspunktet."

Erklæringsteksten vil blive del af det samlede erklæringskatalog (hjælpetabel) i e-TL, som kan anvendes også af de eksterne brugere/anmeldere, herunder system-system-brugere.

For virksomhedspant/erhvervsløsøre gælder særligt, at afgift beregnes afhængigt af om følgende specifikke erklæring afgives - eller ikke er afgivet - i anmeldelsen:

"Nærværende ændring af pantet omfatter alene erhvervsaktiver. Der sker herved ikke skift af pantsætter."

De nøjagtige ekspeditionstyper for virksomhedspant/erhvervsløsøre er oplyst i Bilag 2B side 181-182.

Erklæringerne sendes "til" webservicen Afgiftsberegning som del af de strukturerede sektioner, vist på figuren i starten af afsnit 5.11.1.2.

Tinglysningsafgift	
Afgiftsoplysninger	
Pålydende nyt lån	
Sum indfrieede lån	
Omkostninger indfrieede lån	
Kurstab nyt lån	
Omkostninger nyt lån	
Restgæld indfrieede lån	
Afgiftspligtigt beløb	
Opgørelse (kurs/nominel)	
Valutakode	
Kurstype	
Kursdato	
Dokument references	
Afgiftsbeløb	
Årsag for afvigelse	

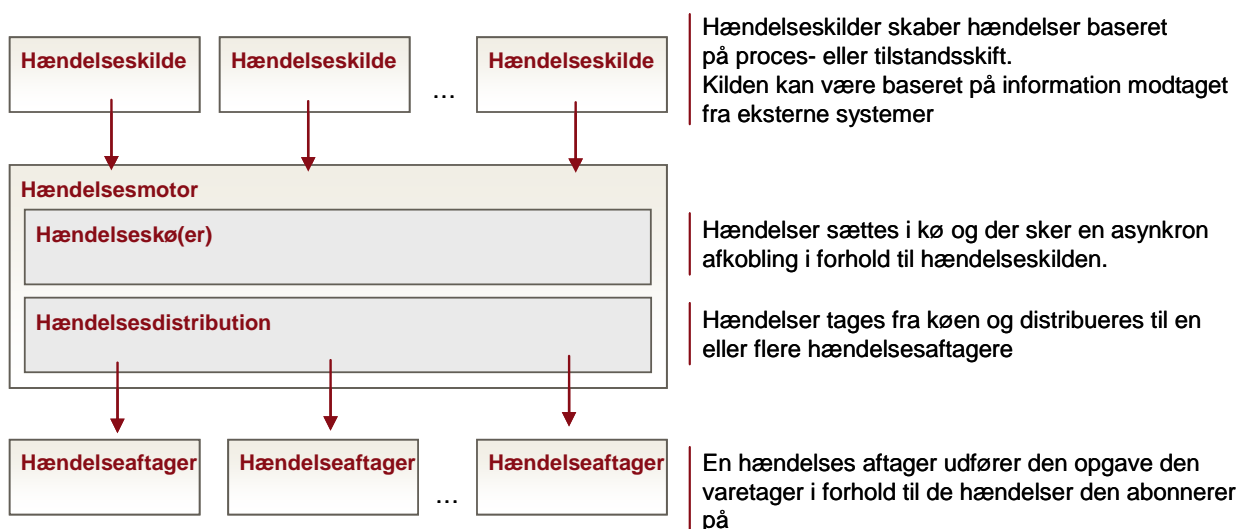
5.12 Hændelsesstyring

5.12.1 Indledning

Overordnet set baserer e-tinglysningsystemet sig på en service-orienteret arkitektur. Dvs. at der anvendes et design-princip om at den funktionalitet der udgør de forretningsmæssige elementer i løsningen udvikles som services og stilles til rådighed for en overordnet procesbeskrivelse gennem en service-bus (Enterprise Service Bus). Formålet hermed er at skabe afgrænsede og uafhængige forretningsmoduler med fleksible anvendelsesmuligheder. Dette betyder også at de enkelte services skal fungere uafhængigt af hinanden og dermed ikke kan basere sig på antagelser om gensidig kendskab og eksistens.

En af de centrale mekanismer til at understøtte sådan en afkobling er anvendelse af et hændelses-koncept. Når begivenheder af forretningsmæssig karakter indtræffer ved afviklingen af en service så har denne service ikke ansvaret for, og dermed ikke til opgave, at udføre evt. afledte handlinger. I stedet signaleres begivenheden ved at udløse en forretningshændelse og ansvaret for den videre udførelse af forretningsmæssigt afledte opgaver delegeres til et centralt hændelsesmodul.

Den generelle arkitektur for hændelsesmodulet er beskrevet ved nedenstående figur.



Når en forretningshændelse udløses vil den blive registreret i en hændelseskø. Denne kø danner den asynkrone afkobling mellem kilden til en hændelse og den eller de aftagere der skal reagere på hændelsen. Formålet med denne asynkrone afkobling er at tillade den proces der er hændelseskilde at forsætte sin behandling selv om hændelsestagerne kortvarigt ikke kan følge med til at afvikle de afledte processer i den takt hændelserne måtte opstå. Det kan eksempelvis være relevant ved forsendelse af meddelelser til eksterne systemer, hvor de underliggende transmissionsprotokoller kan involvere betydelige tidsvinduer for timeout og gentagelsesforsøg for at etablere forbindelser mellem systemerne. Denne afkobling sikrer at den proces der er hændelseskilde (f.eks. en prøvelse af et anmeldelsesdokument) ikke blokeres af eventuelle problemer i relation til hændelsestager (f.eks. forsendelse af e-mail eller webservice kald). Hvis det ikke lykkes for en hændelsestager at gennemføre sine operationer vil den foretage en forretningslogging af dette forhold.

Tinglysningsystemet vil have et antal hændelsestager, heriblandt:

- Forretningslogger: Alle de forretningshændelser der udløses vil blive registreret i en log over forretningshændelser. Dette kan betragtes som en hændelsestager der reagerer på samtlige forretningshændelser og hvis eneste funktion er at logge hændelsen.
- Forsendelse af meddelelser til interessenter og eksterne systemer: De forretningshændelser der kræver at der skal udsendes meddelelser vil udløse de relevante hændelsestager, der

under anvendelse af de services der stilles til rådighed af forsendelsesmodulet, gennemfører disse forsendelser.

- Notifikationer i henhold til valgfrie abonnementer (se nedenfor)

Ud over de ovenfor nævnte hændelsestager vil denne hændelsesmekanisme også blive brugt til at udløse relevante asynkrone interne processer i tinglysningssystemet, herunder også mere batch-orienterede processer.

Når en hændelse udløses så vil der, ud over identifikation af hvilken type forretningshændelse der er tale om, også blive videregivet en kontekst i form af et eller flere data-objekter der karakteriserer årsagen til hændelsen. Denne kontekst vil blive videregivet til de hændelsestager der skal notificeres om hændelsen og disse hændelsestager kan således operere på grundlag af disse data. Udover blot at blive videregivet som datagrundlag til den afledte proces så kan der også foretages filtrering på disse data-objekter således at afledte processer kun startes hvis bestemte betingelser knyttet til konteksten er opfyldt.

Hændelseskilder kan også relateres til begivenheder uden for tinglysningsystemet og således fremadrettet anvendes til at integrere til de data-leverancer og synkroniseringer der skal foregå i forhold til eksterne systemer.

5.12.2 Abonnementer

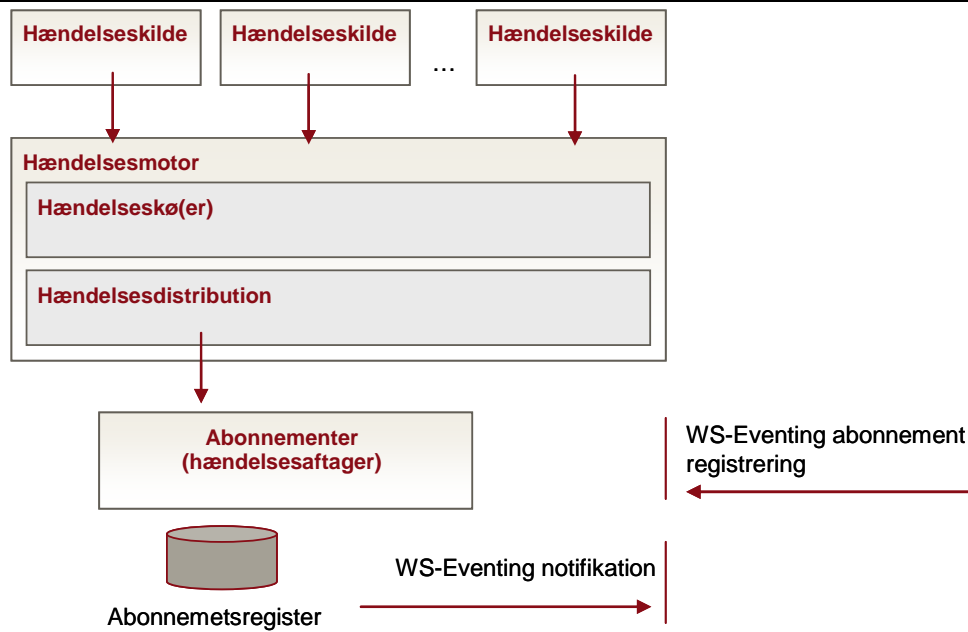
Det vil være muligt for interessenter at anmode om en orientering når der udføres tinglysningsaktivitet i forhold til konkret identificerede tinglysningsobjekter. Dette opnås ved at tegne abonnement. Et abonnement defineres af:

- Det konkrete tinglysningsobjekt hvorpå man ønsker at følge tinglysningsaktivitet. Der kan abonneres på tinglysningsobjekter fra alle tingbøger.
- En identifikation af hvilken/hvilke aktiviteter i forhold til det valgte tinglysningsobjekt man ønsker notifikation om. De mulige aktiviteter vil afhænge af hvilken type tinglysningsobjekt der er valgt (ejendom, bil, person, ...) og svarer til de ekspeditionstyper der kan foretages i relation til tinglysningsobjektet. Ekspeditionstyperne kan evt. grupperes således at det eksempelvis vil være muligt at tegne abonnement på al pant-relateret aktivitet for en ejendom.
- En registrering af hvortil notifikationer skal sendes.

For de interessenter der anvender system-system ordningen vil abonnementsmekanismen basere sig på principperne i det oplæg til standarder der findes for WS-Eventing og WS-Addressing. Disse standarder vedrører hhv. hvordan abonnementer registreres og udløses samt hvordan modtageren af notifikationer udpeger den service der skal modtage notifikationer vedrørende et abonnement. Indholdet i den notifikation der sendes vil være formateret i struktureret XML.

For interessenter der opretter abonnement via portalen vil notifikationer blive udsendt til en e-mail adresse der oplyses i forbindelse med oprettelse af abonnementet. Indholdet i den e-mail der sendes vil være formateret i læsbar tekst

Det modul der forvalter disse abonnementer vil fungere som hændelsestager som vist på nedenstående figur:



Når en hændelse udløses vil de registrerede abonnemeter blive undersøgt og notifikationer vil blive udsendt hvis et eller flere abonnemeter er matches af hændelsen.

Som udgangspunkt antages det at et abonnement løber indtil den interessent der har oprettet det eksplicit afmelder abonnemeter.

5.13 Forsendelsesmodul

5.13.1 Indledning

Forsendelsesmodulet samler de services der anvendes til at *opbygge, formatere og distribuere* dokumenter til brugerne af det elektroniske tinglysningsystem. Dokumenter skal i denne sammenhæng opfattes som en bred definition af de meddelelser og svar der skal kommunikeres til forskellige interessenter som resultat af anmeldelser og forespørgsler. Der er således tale om et antal forskellige dokumenttyper (kommunikationer med forskellige formål) i et antal forskellige formater (XML, PDF, HTML, ...) ad forskellige kanaler (webservice, e-mail, e-Boks, brev, ...).

5.13.2 Overordnede services

Som antydnet underopdeles de services som stilles til rådighed i forsendelsesmodulet i tre overordnede grupper. Dette har til formål at sikre den nødvendige granularitet af services i forhold til de processer der defineres i e-tinglysningsystemet. Derudover skal det sikre fleksibilitet i forhold til på simpel og struktureret vis at foretage fremtidige udvidelser mht. dokumenttyper, formater og distributionskanaler.

5.13.2.1 Opbygning

Opbygningen af dokumenter beskriver den indholdsmæssige sammensætning af et dokument og relaterer således til dokumenttypen. Hver dokumenttype vil være defineret af en skabelon, dvs. en indholdsmæssig ramme, der fastlægger og strukturerer indholdet i et konkret dokument. Denne skabelon kan ud over strukturen også definere nogle statiske elementer af et dokument, enten i form af fast definerede tekster eller referencer til grafiske objekter der skal indgå i dokumentet. Et konkret dokument *opbygges* således ved at en skabelon kombineres ("flettes") med et struktureret dataobjekt der beskriver den dynamiske del af indholdet i dokumentet, svarende til den aktuelle kontekst hvor dokumentet bliver dannet. Resultatet af denne fletning er et indholdsmæssigt komplet dokument på en struktureret logisk form men endnu uden beskrivelse af hvordan det skal formateres (præsenteres) for modtageren.

5.13.2.2 Formatering

Ved *formateringen* af et dokument fastlægges hvordan et dokument der er opbygget efter ovenstående principper skal præsenteres for modtageren. Som udgangspunkt for alle øvrige formateringer kan dokumenter formateres som XML dokumenter. Denne form fastholder den strukturerede form af indholdet i dokumentet og er derfor også det naturlige format til anvendelse ved system-system kommunikation.

I modsætning til XML formateringen er formålet med alle øvrige formater at præsentere dokumentet i et for mennesker læsbart layout. Opbygningen af disse formater vil foregå med afsæt i XML formateringen af dokumentet og basere sig på XSL transformationer (XSLT) og i det omfang det er muligt vil der blive gjort brug af eksisterende, åbne og tilgængelige implementationer af sådanne transformationer. I forhold til generering af PDF dokumenter og dokumenter til print vil anvendelse af standarden XSL Formatting Objects (XSL-FO) og implementationen Apache FOP² blive taget i betragtning.

De XSL transformationer der opbygges til at understøtte formateringen af dokumenter vil blive versioneret således at det er muligt hen over e-tinglysningsystemets levetid at foretage ændringer i

² Apache FOP (Apache Formatting Object Processor) er en open source implementation der understøtter et antal forskellige præsentationsformater men har primært fokus på PDF. Yderligere information er tilgængelig på <http://xmlgraphics.apache.org/fop>.

formateringen og det vil ligeledes konkret for anmeldelser være muligt at fastholde hvilken version der var gældende ved oprettelsen af anmeldelsen. Transformationerne vil også via webservices blive gjort tilgængelige for eksterne brugere under *system-system ordningen*, der således kan vælge i egne systemer at gøre brug af disse transformationer til at præsentere de XML dokumenter de modtager fra e-tinglysningssystemet i et læsbart format.

I nogle sammenhænge skal de dokumenter der genereres i e-tinglysningssystemet underskrives med Tinglysningsrettens digitale signatur. Det drejer sig generelt om XML dokumenter men vil også involvere formelt attesterede dokumenter der er rekvireret mod betaling der formateres i PDF. Derved sikres autenticiteten og den indholdsmæssige integritet af dokumentet efter det har forladt e-tinglysningssystemet. Det skal bemærkes at denne signatur i relation til PDF vil være knyttet til selve PDF dokumentet, og ikke til den forsendelse der indeholder PDF dokumentet. Det betyder at hvis dokumentet sendes med e-mail så er det ikke selve e-mailen der er digitalt signeret, men det vedhæftede PDF dokument. Derved sikres at signaturen følger dokumentet selv om det anvendes separat fra den e-mail der blev brugt til distribution. Digital signering af formaterede dokumenter udgør en selvstændig service der dog knytter sig til formateringen af dokumenter.

5.13.2.3 Distribution

Den sidste kategori af services vedrører distribution af dokumenter. Overordnet set kan dokumenter distribueres ad tre kanaler:

- System-system kommunikation
- Formidling gennem portalerne
- Direkte forsendelse – elektronisk forsendelse eller traditionel brevfor sendelse

System-system kommunikation anvendes i forhold til de brugere der er registrerede mht. til *system-system ordningen* og som anvender denne snitflade til at fortage forespørgsler og anmeldelser. Denne kommunikation baserer sig på webservice kald og udveksling af dokumenter i XML format. I forbindelse med forespørgsler (eksempelvis på akter og attester) vil dette foregå som et synkront svar fra e-tinglysningssystemet på en forespørgsel initieret af den eksterne bruger. Ved indsendelse af en anmeldelse modtager den eksterne bruger umiddelbart blot en kvittering der bekræfter modtagelse og en initial status for anmeldelsen. Al efterfølgende kommunikation vedrørende anmeldelsen initieres asynkront af e-tinglysningssystemet i takt med at forskellige hændelser i behandlingsforløbet udløses og det er således nødvendigt at der til den eksterne bruger registreres oplysninger om hvortil meddelelser fra e-tinglysningssystemet skal sendes. I henhold til kravspecifikationen og den efterfølgende afklaring³ er princippet således at der i forbindelse med oprettelsen af en *system-system ordning* for en ekstern bruger registreres et (eller evt. flere) ”endpoint” i form af en webservice som modtager af denne asynkrone kommunikation. Derudover kan anmelderen til en konkret anmeldelse tilføje en eller flere e-mailadresser (i kravspecifikationen betegnet *separatadresser*) hvortil alle udløste meddelelser også skal sendes. Disse vil blive behandlet efter principperne beskrevet nedenfor vedrørende *Direkte forsendelse*.

Formidling gennem portalen vedrører brugere der foretager anmeldelser eller forespørgsler gennem portalen. Når brugeren igangsætter en forespørgsel eller anmeldelse gennem portalen så vil meddelelser fra e-tinglysningssystemet også blive kanaliseret tilbage gennem portalen. I forhold til forespørgsler så vil de resulterende dokumenter blive præsenteret direkte for brugeren direkte i portalen. For anmeldelser vil brugeren blive præsenteret for en kvittering for modtagelse og de efterfølgende kommunikationer om status og det endelige svar vedrørende tinglysning vil blive gjort tilgængelige gennem brugerens egen sagsmappe ”Mine Tinglysninger” på portalen. Som det er tilfældet ved *system-system kommunikation* så kan der også ved anmeldelser fortaget gennem portalen tilføjes en eller flere e-mailadresser (*separatadresser*) hvortil udløste meddelelser også skal sendes.

³ Jf. svar på forespørgsel i e-mail fra Henrik Hvid, 12-02-07 ”RE: Spørgsmål til afklaring vedrørende e-Tinglysning”

Direkte forsendelse anvendes til at distribuere dokumenter der formateres i et læsbart format. Som beskrevet ovenfor involverer dette eksempelvis distribution af e-mails til separatadresser i forbindelse med anmeldelser. Derudover skal der foretages forsendelse med traditionelt brev eller til e-Boks f.eks. i relation til anmelderordningen hvor der skal foretages underretning af adkomsthaver. I forhold til de forskellige forsendelseskanaler anvendes følgende formater:

- **e-mail:** Indholdet i en e-mail kan bestå af et dokument i simpel tekst samt af vedhæftede dokumenter (attachments) i form af PDF dokumenter. I nogle sammenhænge vil e-mails fra e-tinglysningsystemet blot indeholde simple orienterende tekstbeskeder, mens der i andre tilfælde vil være tale om mere formelle dokumenter. I sidstnævnte tilfælde vil det formelle dokument være et vedhæftet PDF dokument, mens e-mailens tekstindhold har karakter af et orienterende følgebrev der bl.a. kan beskrive hvordan vedhæftede dokumenter kan vises og anvendes. Der kan ikke svares på udsendte e-mails.
- **e-Boks:** Det eneste format der accepteres for leverancer til e-Boks er PDF. Alle forsendelser fra e-tinglysningsystemet til e-Boks vil derfor være i PDF format.
- **brev:** Brevforsendelser vil som udgangspunkt blive betragtet som en udskrift af dokumentet i elektronisk form (PDF) med efterfølgende kuvertering og distribution. Til den udskrevne version tilføjes evt. enkelte tekstuelle og grafiske elementer som f.eks. modtagers navn og adresse eller strekkoder til anvendelse ved den automatiserede kuvertering, men mht. til indhold og layout modsvarer udskriften den tilsvarende PDF dokument.

5.13.3 Integration til print-center

I relation til forsendelser via brev og til e-Boks anbefaler CSC et samarbejde med en ekstern print- og distributions-leverandør. Disse to kanaler udgør i forhold til e-tinglysningsystemet en samlet overordnet distributionskanal da valget mellem modtagelse som brev eller i e-Boks ikke kan træffes i portalen men ved registreringer direkte hos e-Boks. Det skal således prøves i forhold til hver enkelt forsendelse om modtageren har oprettet abonnement på den konkrete forsendelse hos e-Boks og i henhold til dette skal forsendelsen enten afleveres til e-Boks eller printes og sendes som brev.

Opgaven vedrørende printning og forsendelse af breve samt integration til e-Boks, forvaltning af abonnementsregistreringer og distribution til e-Boks udgør en meget velafgrænset service i forhold til e-tinglysningsystemet. Denne service kan med fordel delegeres til en specialiseret service-leverandør der råder over den nødvendige tekniske og ressourcemæssige infrastruktur og som er i stand til at levere den nødvendige ydelse som en relativ standardiseret service.

Udestående: I relation til e-Boks skal der træffes valg om hvilke konkrete forsendelser Tinglysningsretten ønsker at tilbyde på elektronisk form og der skal oprettes en leverandør-aftale med e-Boks. Den enkelte borger har herefter mulighed for at tilvælge en eller flere af disse forsendelser til modtagelse i sin e-Boks.

5.14 Overvågning og status

Det samlede systemkompleks overvåges som en del af den almindelige drift i CSC's driftcenter. Her findes generelle værktøjer til overvågning af hardware, infrastrukturkomponenter samt applikationerne installeret i infrastrukturen. Informationer fra disse overvågningsværktøjer er som udgangspunkt kun tilgængelige for driftspersonalet.

Ud over den detaljerede driftsmæssige tekniske overvågning stiller e-tinglysningsystemet information til rådighed for eksterne parter.

Den information der stilles til rådighed kan opdeles i 2 hovedkategorier:

1. Teknisk information og status
2. Forretningsmæssig information og status

Begge typer af information kommunikerer via to kanaler.

Den ene kanal er den eksterne portal, som vil indeholde sider som fortæller om teknisk og forretningsmæssig status på e-tinglysningsystemet.

Den anden kanal er hændelsessystemet, som vil kunne distribuere statusinformation af teknisk og forretningsmæssig karakter til system-system partnere. Information der distribueres via hændelsessystemet vil være i XML og vil egne sig til automatisk processering i det modtagende system.

Den konkrete information, der distribueres er ikke fastlagt endnu.

Et eksempel på teknisk statusinformation kunne være information om nedlukning af e-tinglysningsystemet, således at eksterne vil være ajour med hvornår der er planlagte nedlukninger.

Forretningsmæssig statusinformation kunne være overordnet statistikinformation der informerer om gennemsnitlige ekspeditionstider for de enkelte ekspeditionstyper.

Bemærk! Statusinformation vedrørende en konkret anmeldelse hører *ikke* ind under beskrivelsen af statusinformation i dette afsnit. Denne type statusinformation håndteres som en del af tinglysningsprocessen og vil blive kommunikeret til anmelderen og andre interessenter.

5.15 Statistikmodul

5.15.1 Logning

5.15.1.1 Logning af informationer vedr. sagsbehandling

For hvert procestrin i workflowet lige fra handlingerne vedr. generering af en anmeldelse på den eksterne portal til afslutning på anmeldelsen, logges information om:

- Ekspeditionstype
- Tidspunkter (dato/klokkeslet) for påbegyndelse og afslutning af individuelle processkridt, og dermed også ventetider.
- Involverede sagsbehandlere (baseret på deres handlinger – fx hvem har udført hvilke handlinger vedr. en given manuel ekspedition.
- Status for de enkelte prøvelser undervejs i processen.

På baggrund af denne information, vil man kunne udtrække alt relevant information om sagsbehandling, både til optimering af ressourceforbrug, og ift. at levere relevant information om behandlingstider til eksterne interessenter.

For at muliggøre live visning af visse statistiske oplysninger, kan det være relevant at udarbejde disse løbende som kummulative statistikker. Ved afslutning af anmeldelser, vil det eksempelvis være relevant at notere ekspeditionstype, samlet tid for gennemførelse af prøvelsen osv. til en separat statistik, så denne information kan tilgås fra applikationen live.

5.15.1.2 Logning af information vedr. e-akten

Statistik, som udtrækkes på basis af data fra e-akten, udtrækkes via det samme datagrundlag som for de summariske oplysninger. Dette vil kunne definere visse begrænsninger på omfanget af de statistikker, som vil kunne udtrækkes heraf.

5.15.2 Statistiktyper

5.15.2.1 Online statistikker

Online statistikker, hvor resultatet foreligger umiddelbart, kan omhandle enten fx brugsstatistik (fx. fordeling af anmeldelser på ekspeditionstyper), hvor data er opsamlet løbende, eller andre typer statistik, som kan dannes ved forholdsvis simple databaseopslag. Mængden af sager i kø, fordelt på ekspeditionstype, eller fx. på medarbejder, er også eksempler på online statistikker.

5.15.2.2 Schedulerede statistikker

Statistikker, som er ressourcekrævende at få udført, scheduleres til kørsel om natten for ikke at belastte systemet i dagtimerne. Det vil blive vurderet for hver enkelt statistiktype, om kørselen er så omfattende, at det vil være nødvendigt at afvikle den scheduleret.

5.15.2.3 Specialkørsler

Det vil endvidere være muligt at danne statistikker, som har sådanne frihedsgrader, at de for brugeren vil blive opfattet som specialkørsler. I praksis vil disse statistikker blive opbygget kontrolleret, således at brugeren kan sammensætte statistikkerne med input data, der ligger inden for et vist parameterinterval, men på en måde, så brugeren ikke ved en fejl kommer til at danne en statistik, som tapper systemet for ressourcer.

5.15.3 Rettigheder

Rettigheder ifbm. statistikkørsler tildeles efter, om brugeren skal have adgang til ledelsesinformati-
oner og om brugeren har fået tildelt særlig adgang til igangsætning af Schedulede statistikkørsler.
Rettigheder bliver implementeret som en integreret del af den generelle rettighedsstyring.

5.15.4 Processen for etablering af statistik- og rapportmodulet

Det kræver en forretningsmæssig analyse, som DSS skal have foretaget i samarbejde med CSC, for
at få defineret det præcise behov for statistikker og udtræk af rapporter. Analysen vil med fordel
kunne gennemføres som en integreret del af udviklingsforløbet.

5.16 DIBS betalingssystem

5.16.1 DIBS

Til håndtering af online indbetalinger af rets- og tinglysningsafgifter i den eksterne portal anvendes DIBS (Dansk Internet Betalings System www.dibs.dk).

DIBS er en betalingsløsning som bl.a. understøtter online betaling med dankort, internationale kreditkort og netbankbetaling.

DIBS udbyder forskellige moduler afhængig af, hvilke betalingsmetoder der ønskes understøttet. F.eks. løsningen "Basis", som understøtter Dankort & Visa/Dankort, eDankort og Netbankbetaling. "Premium" løsningen har desuden understøttelse for internationale kreditkort. (Diners, American Express, MasterCard etc.)

5.16.2 Løsningsmodel

For at have maksimal kontrol over design og workflow i portalen vælges en løsning, som giver mulighed for at udvikle og hoste de sider i portalen som vedrører betalingen i modsætning til løsningsmodeller, hvor betalingssystemets standardskærm billeder/flow anvendes. Således foregår transaktionsforespørgsler direkte mellem e-TL portalens og betalingssystemets servere. Det er derfor en forudsætning, at der anskaffes et SSL-certifikat (Secure Socket Layer), således at portalbrugernes opgivelse af kreditkortoplysninger ikke bliver kompromitterede. Opgaven med at anskaffe SSL-certifikatet foretages af CSC

Dermed skal der i portalen etableres brugerinterface til at angive valg af betalingsmetode, indtastning af kontonr, udløbsdato og kontrolcifre. Ved brugerens bekræftelse af betalingen videregives oplysningerne som en autorisationsforespørgsel til DIBS-serveren, som derefter returnerer et svar i form af afvisning eller accept.

5.16.3 Forudsætninger

For at håndtere online betalingstransaktioner via DIBS skal der laves en aftale mellem DSS og DIBS. Aftalen skal som minimum understøtte online-betaling med de relevante danske og internationale betalings- og kreditkort. Desuden skal der i aftalen være understøttelse af netbank-betaling, mulighed for integration til egne portalsider og refusion af allerede gennemførte betalinger.

For at benytte muligheden for netbankbetaling forudsættes at der er oprettet en aftale og en konto med det enkelte pengeinstitut.

Bemærk: Desuden kræver pengeinstitutterne som udgangspunkt, at deres netbetalingslogo forefindes på portalens forside!!

Det forudsættes, at der anskaffes et SSL-certifikat, så portalens betalingssider eller portalen som helhed anvender SSL.

Ved anvendelse af DIBS' server-til-server autorisation kræves en underskrevet erklæring om at DSS ikke lagrer følsomme informationer på portalens servere.

5.16.4 Betalings- og Kreditkortbetaling

Ved kreditkortbetaling foregår kommunikationen mellem e-TL portal serveren og DIBS-serveren via DIBS API, som udstiller betalingssystemets funktioner.

Følgende DIBS transaktionstyper skal anvendes i portalen:

- *Autorisation* - Kontrol af oplysninger om kort og dækning på den tilhørende konto.
- *Cancel* - Annullerer en autorisation.
- *Capture* - Den egentlige betaling (flytning af penge mellem konti).
- *Refundering* - Tilbageførsel af allerede gennemførte betalinger.

5.16.4.1 Autorisation

Autorisationen udfører en kontrol af kortoplysningerne og reserverer et beløb på portalbrugerens konto til senere overførsel. Kontrolfunktionen kan kaldes fra HTML formularen på portalen eller direkte fra portal serveren vha. et HTTPS-kald (SSL). Nedenfor er anført de væsentligste parametre og returværdier ved kald til DIBS. Der skal tages højde for, at der i fremtiden kan forekomme tilføjelser til både parametre og returværdier, hvor transaktionsnummer anvendes til efterfølgende capture transaktion.

Parametre i autorisationskaldet

Obligatoriske:

- *merchant* - Firmaidentifikation (Merchant-nummer) 7-cifret tal
- *amount* - Beløb
- *currency* - Valutaangivelse i ISO4217 format (Dkk = 208)
- *cardno* - Kortnummer (11-19 cifre afh. af korttype)
- *expmon* - Udløbsmåned (2 cifre)
- *expyear* - Udløbsår (2 cifre)
- *orderid* - Ordrenummer eller anden identifikation (numerisk og/eller alfanumerisk 50 tegn)
- *textreply* - Angivelse af om svar skal gives i simpel tekst ("textreply" eller tom)
- *fullreply* - Angivelse af om man ønsker fullreply med ("fullreply" eller tom virker kun sammen med textreply)

Valgfrie:

- *cvc* - Kreditkortets kontrolnummer
- *uniqueoid* – Hvis dette felt er sat må der ikke være 2 ens ordrenumre – i så fald afvises transaktionen.
- *capturenow* – Anvendes ved "instant capture", øjeblikkelig overførsel.
- *account* – identificerer en bestemt indbetalingskonto, hvis der er oprettet flere konti hos DIBS
- *cardtype* – kan afgrænse de tilladte korttyper.

Returværdier ved godkendt betaling

Obligatoriske:

- *transact* - Transaktionsnummer tildelt af DIBS (6-cifret tal)
- *status* - Transaktionsstatus ("ACCEPTED" alfanumerisk)

Valgfrie

- *suspect* - Returnerer "true", hvis DIBS svindelkontrol har mistanke om misbrug.
- *severity* - (heltal) karakterisering af hvor tvivlsom transaktionen er vurderet.
- *orderid* - samme som kaldt parameter med samme navn

Returværdier ved afvist betaling

Obligatoriske:

- *status* - ("DECLINED" alfanumerisk)
- *reason* - (heltal) Fejlkode som angiver årsagen til afvisningen

5.16.4.2 Cancel

Når der er foretaget en gyldig autorisation af kreditkortet kan autorisationen annulleres vha. kald til cancel-funktionen. Ved samme lejlighed frigives det beløb, som blev reserveret i forbindelse med autorisationen.

Parametre (obligatoriske)

- `merchant` - Firmaidentifikation
- `transact` - Transaktionsnummer for tidligere autorisation.
- `textreply` - Angivelse af om svar skal gives i simpel tekst ("textreply" eller tom)

Returværdier ved korrekt gennemført transaktion

- `status` - "ACCEPTED"
- `transact` - Transaktionsnummer for tidligere autorisation.
- `cardtype` - Korttype (kode)

Returværdier ved afvist transaktion

- `status` - "DECLINED"
- `reason` - fejlkode med tilhørende årsagsforklaring

5.16.4.3 Capture

Når der er foretaget en gyldig autorisation af kreditkortet kan capture funktionen kaldes med autorisationens transaktionsnummer som parameter. Derved foretages den egentlige pengeoverførsel mellem portalbrugers konto og de konti som DSS anvender til indbetaling af rets- og tinglysningsafgifter.

Parametre i autorisationskaldet (obligatoriske)

- `merchant` - Firmaidentifikation
- `amount` - Beløb (der kan angives beløb som er mindre end det autoriserede)
- `transact` - Transaktionsnummer for tidligere autorisation.
- `orderid` - Ordrenummer eller anden identifikation (numerisk og/eller alfanumerisk 50 tegn)

Returværdi

- `result` - 0: transktionen er gennemført, ≠ 0: result indeholder fejlkode til årsagsbeskrivelse.

5.16.4.4 Refundering

Hvis der ved en tinglysning skal foretages refusion af evt. retsafgifter i forbindelse med relaterede forespørgsler kaldes refund transaktionen i DIBS-API.

Parametre i refusionskaldet (obligatoriske)

- `merchant` - Firmaidentifikation
- `amount` - Beløb (der kan angives beløb som er mindre end det autoriserede)
- `transact` - Transaktionsnummer for tidligere autorisation.

- `orderid` - Ordrenummer eller anden identifikation (numerisk og/eller alfanumerisk 50 tegn)
- `textreply` – Hvis feltet ikke er tomt returneres simpelt tekstsvaret

Sikkerhed

For at sikre at andre ikke kan refundere, skal der før transaktionskaldet angives brugernavn & password. Brugernavn og password er de samme som der anvendes for adgang til DIBS-administrationen. Brugeroplysningerne kan indsættes i HTTP-headeren.

Returværdi

- `reason` - 0: transaktionen er gennemført, \neq 0: transaktionen blev afvist, reason indeholder fejlkode til årsagsbeskrivelse.

5.16.5 Netbankbetaling

DIBS giver mulighed for, at der kan foretages netbankbetalinger fra udvalgte pengeinstitutter. Det er således muligt at dirigere brugeren direkte til dennes netbank. Transaktionen udføres derefter mellem brugeren og banken via dennes netbank brugerinterface.

Parametre i kald til netbank

Obligatoriske:

- `merchant` - Firmaidentifikation 7-cifret tal
- `amount` - Beløb
- `currency` - Valutaangivelse i ISO4217 format (kun Dkk kan benyttes = 208)
- `orderid` - Ordrenummer eller anden identifikation (numerisk og/eller alfanumerisk 50 tegn)
- `accepturl` - URL på side der skal vises hvis købet godkendes
- `declineurl` - URL på side der skal vises hvis købet afvises
- `cancelurl` - URL på side der skal vises hvis købet annulleres

Returværdier ved godkendt betaling

Obligatoriske:

- `transact` - Transaktionsnummer tildelt af DIBS (6-cifret tal)
- `status` - Transaktionsstatus ("ACCEPTED" alfanumerisk)

Valgfrie

- `suspect` – Returnerer true, hvis DIBS svindelkontrol har mistanke om misbrug.
- `severity` - (heltal) karakterisering af hvor tvivlsom transaktionen er vurderet.
- `orderid` – samme som kaldt parameter med samme navn

5.16.6 Onlinebetaling i den eksterne portal

Som af del af processen med at opbygge og indsende et dokument til tinglysning på den eksterne portal, indgår det skridt som afkræver betaling af tinglysnings- og retsafgift.

Som udgangspunkt præsenteres brugeren for det beløb som systemet har beregnet på baggrund af den anmeldelse, som brugeren har udformet på portalen. Beløbet kan af brugeren rettes hvis denne ikke er enig i beregningen af afgiften. I det tilfælde vil brugeren blive gjort opmærksom på at uenigheden om afgiften vil blive overgivet til afgiftsmyndigheden.

Hvis systemet afgør ud fra brugerens certifikat at denne repræsenterer en virksomhed under storkundeordningen, vil brugen få valgmuligheden om at benytte storkundeordningen, eller betale kontant ved brug af betalingskort.

Brugere som ikke kan identificeres som hørende til en virksomhed under storkundeordningen vil blive afkrævet betaling via betalingskort.

5.16.6.1 Betalings- og Kreditkortbetaling brugergrænseflade

Der vises en side hvor brugeren skal angive kreditkorttype, kreditkortnummer, udløbsdato og evt. kontrolcifre. Hvis brugeren vælger at acceptere betalingen vises en side med summariske oplysninger om beløb og transaktionsbeskrivelse. Hvis brugeren bekræfter betalingsoplysningerne foretages et transaktionskald til DIBS, hvorved kreditkortet forsøges autoriseret og i tilfælde af godkendelse reserveres beløbet på brugerens konto.

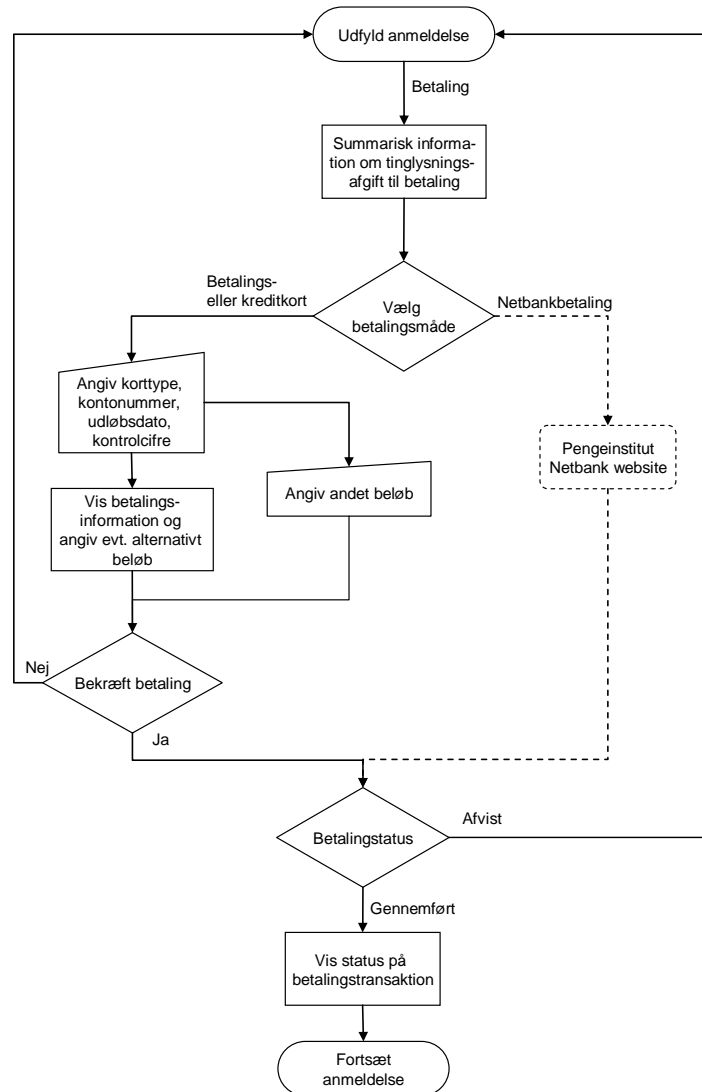
Der vises en side med oplysning om betalingstransaktionens forløb i form af godkendelse eller afvisning og dennes årsag.

5.16.6.2 Netbankbetaling brugergrænseflade

Når der vælges netbankbetaling åbner browseren pengeinstituttets netbank sider, hvor brugeren autoriserer sig på normal vis og foretager betalingen vha. pengeinstituttets netbank brugergrænseflade.

5.16.7 Betaling af tinglysningsafgift

Når en anmeldelse til tinglysning er udfyldt i tilstrækkelig grad til, at der kan beregnes en tinglysningsafgift, har brugeren – det være sig anmelder eller anden part - mulighed for at indbetale det beregnede beløb via online betaling, enten vha. kreditkort eller netbankbetaling.



Brugeren får en oversigt over de enkelte beløb, der tilsammen udgør omkostningerne for den ønskede transaktion. Dernæst skal brugeren tage stilling til, hvilken betalingsform der skal anvendes. Der kan vælges mellem to betalingsformer:

- Kreditkort online-betaling
- Netbank-betaling

Selve betalingstransaktionen udføres som beskrevet i afsnit *Betalings- og Kreditkortbetaling brugergrænseflade* og *Netbankbetaling brugergrænseflade*. Når betalingen er gennemført returneres til siden hvorfra betalingstransaktionen blev valg.

Selve overførslen af beløb fra brugerens konto (*capture transaktion*) udføres først i det øjeblik, hvor anmeldelsen bliver tinglyst. Hvis anmeldelsen derimod afvises, annulleres betalingsautorisationen og beløbsreservationen (*cancel transaktion*).

5.16.7.1 Angivelse af andet beløb

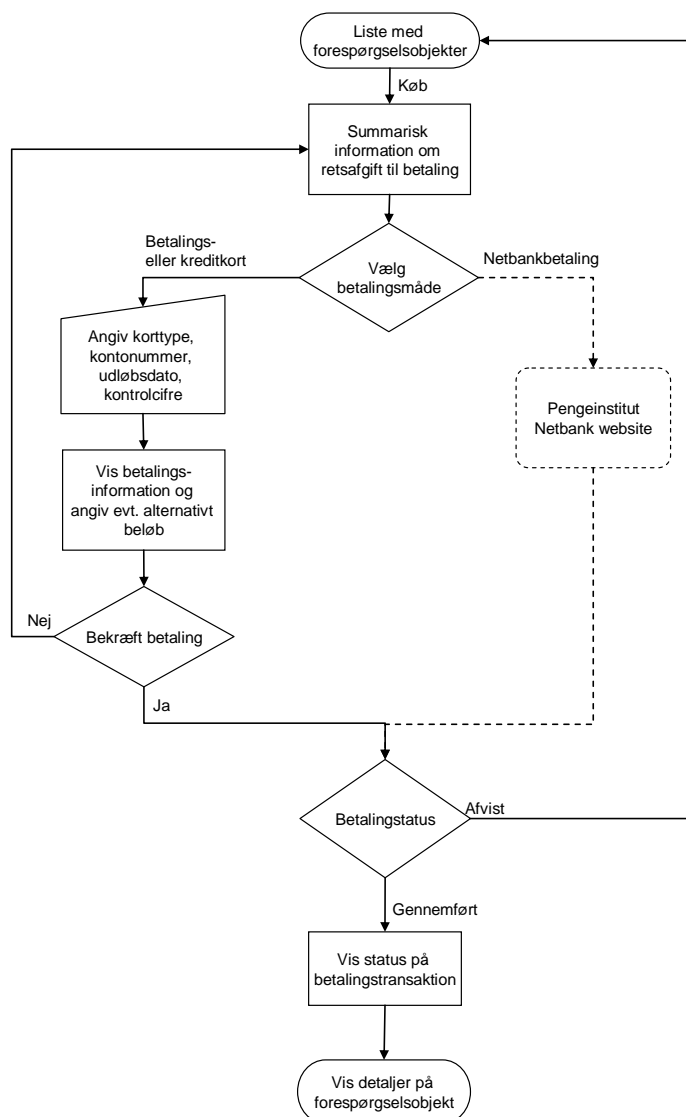
Inden der vælges betalingsmåde kan brugeren vælge at angive et andet beløb end det automatisk beregnede. Derved vises en side, hvor det selvvalgte beløb angives sammen med en tekstuel årsagsforklaring. Hvis brugeren indbetaler et andet beløb end det som foreslås af systemet, gives med-

delelse om at restbeløbet skal indbetales inden 6 hverdage. Hvis beløbet efter 6 hverdage stadig ikke er indbetalt, udtages anmeldelsen automatisk til manuel behandling

5.16.8 Betaling af retsafgift

Forespørgsler på bilbogen og oplysninger om egen person, egen virksomhed eller egen ejendom er afgiftsfri, mens alle andre forespørgsler udløser en retsafgift.

Retsafgiften kan refunderes, hvis forespørgslen inden for 6 arbejdsdage danner grundlag for en efterfølgende tinglysning)



Ved en forespørgsel vises en liste med et eller flere fremsøgte objekter. Hvis detaljeret visning af et objekt fordrer indbetaling af en retsafgift, skal brugeren ”købe” adgang til at se detaljerne. Hvis brugeren således vælger at købe adgang til objektet startes portalens betalingsdel, og der gives mulighed for at vælge mellem betaling via kreditkort eller netbankbetaling.

Selve betalingen udføres som beskrevet i afsnit ”Betalings- og Kreditkortbetaling brugergrænseflade” og ”Netbankbetaling brugergrænseflade”.

Hvis betalingen gennemføres vises detaljerede oplysninger for det valgte objekt.

Hvis betalingen ikke gennemføres vises den oprindelige liste med fremsøgte forespørgselsobjekter.

5.17 Tekstfraser

I e-TL vil der blive anvendt tekstfraser i flere forskellige situationer. Tekstfraserne har til formål at sikre at der anvendes ensartede formuleringer både ved anmeldelse, svar på anmeldelse og ved forespørgsler/oversigter. Udover at sikre en ensartethed giver anvendelsen af tekstfraser også mulighed for at kontrollerne i den automatiske prøvelse kan kontrollere de tekster som indgår i en anmeldelse.

En frase kan udover selve teksten indeholde et antal variable felter, som indgår i teksten. Hver af disse felter er beskrevet med en type (fx tekst eller tal) evt. kombineret en liste af værdier, som kan anvendes. Hvis der er tilknyttet en liste af værdier kan det specificeres om denne liste er udtømmende eller om værdier, som ikke påtræder i listen også kan angives.

Tekstfraser kan grupperes i et antal grupper. Denne gruppering kan benyttes til at angive fraser, som anvendes indenfor samme område. Dette kan fx benyttes til at danne vilkårsmoduler, således kan en frasegruppe være rentevilkår, opsigelsesvilkår, etc.

5.17.1 Typer af fraser

Tekstfrase er en generel betegnelse for forskellige typer af tekster, som benyttes i e-TL. Der er identificeret følgende forskellige typer af fraser.

- Erklæringstekst
- Vilkårstekst
- Fuldmagtstekst
- Meddelelsetekst
- Standardtekst
- Tillægstekst
- Generelle anmærkningstekster

5.17.2 Erklæring

En erklæring er en tekst, som afgives i et tinglysningsdokument. Den er typisk bundet til en af de roller som indgår i dokumentet (fx sælger). Ved at afgive en erklæring tages ansvar for det udsagn som står i erklæringen. En erklæring kan være lovpligtig eller i øvrigt nødvendige for den automatiske prøvelse af tinglysningsdokumentet. For at en erklæring giver mening, så skal den rolle, som afgiver erklæringen have underskrevet tinglysningsdokumentet (enten direkte eller via fuldmagt). Erklæringer anvendes meget i forhold til adkomster, men er relevante på alle områder.

I mange tilfælde skal kontrollerne i den automatiske prøvelse kunne undersøge om helt specifikke erklæringer er afgivet. Dette kræver, at der findes en liste af kendte erklæringer, som der automatisk kan checkes for. En konkret erklæring kan så markeres som værende en given kendt erklæring.

For nogle erklæringer er der specifikke regler for hvornår de skal afgives. Et eksempel på en sådan regel er, at hvis en køber er en virksomhed, så er der visse erklæringer, som skal afgives.

Herudover kan erklæringer kan have følgende indbyrdes afhængigheder

- Nogle erklæringer kan ikke afgives alene, men forudsætter at der allerede er angivet andre erklæringer. Denne afhængighed er hierakisk i flere niveauer.
- Nogle erklæringer er i modstrid med hinanden, og kan ikke optræde sammen

Udestående: Hvis en brugerformular indeholder erklæringer, skal vi være sikre på at anmeldelser der anvender brugerformualren ikke indeholder modstridende erklæringer. Det skal derfor være muligt, for tinglysningsretten i forbindelse med godkendelsen af en brugerformular, at angive erklæringer, der ikke kan angives i anmeldelser der anvender den pågældende brugerformular

5.17.3 Vilkår

Et vilkår er noget, som aftales mellem to eller flere parter i et tinglysningsdokument. Et vilkår forpligter parterne overfor hinanden og vil typisk indeholde gensidige rettigheder. Vilkår anvendes i forhold til hæftelser, ejendomsforbehold og servitutter. Vilkår er delt op i et antal grupper, hvor de enkelte vilkår indenfor den samme gruppe omhandler det samme område. Et eksempel kunne være en gruppe som hedder rentevilkår. Disse grupper af vilkår kaldes også for vilkårsmoduler.

5.17.4 Fuldmagtstekster

En fuldmagtstekst benyttes til at anmelde fuldmagter som del af anmeldelsen af et tinglysningsdokument, som ikke selv er en fuldmagt. Et pantebrev kan eksempelvis indeholde en fuldmagtstekst, som giver kreditor fuldmagt til at foretage visse fremtidige tinglysninger (påtegninger og afløsning) på det pågældende pantebrev. Hver fuldmagtstekst har en specifik betydning i forhold til hvilket tinglysningsdokument det indgår i. Angivelsen af en fuldmagtstekst giver anledning til at der oprettes en konkret fuldmagt med et foruddefineret indhold. En fuldmagt oprettet via en fuldmagtstekst til altid kun give fuldmagt til det konkrete tinglysningsdokument, som anmeldes. Dvs. give fuldmagt til at påtegne eller afløse det anmeldte tinglysningsdokument.

Initielt, vil der blive oprettet nogle få standardfuldmagtstekster. Disse skal være synlige på portalen, således at hvis en bruger ønsker at oprette en fuldmagt som skal tinglyses som en del af en anmeldelse, skal den pågældende præsenteres for de fuldmagter som nu en gang kan anvendes ved den pågældende type af anmeldelse.

5.17.5 Meddelelsetekster

En meddelelsetekst er en specifik tekst, som skal angives i tinglysningsdokumentet (hæftelser og ejendomsforbehold) hvis det indeholder angivelse af en eller flere meddelelshavere. Teksten beskriver de præcise forhold om at være meddelelshaver. Der findes kun én meddelelsetekst. Dette tekst inddateres og vedligeholdes på den interne portal.

5.17.6 Standardtekster

En standardtekst er en frase, som benyttes ved tilbagemeldinger på tinglysning og ved visning af status for tinglysning, dvs. til påtegning og anmærkninger. Standardtekster anvendes i stor stil i det eksisterende tinglysningsystem, med dels et centralt sæt af standardtekster som kan benyttes af alle de eksisterende retskredse dels et lokalt sæt af standardtekster for hver retskreds. I det eksisterende system indsætter den enkelte sagsbehandler de relevante standardtekster ved behandling af en anmeldelse. I det nye tinglysningsystem vil standardteksterne blive indsat automatisk af systemet via kontroller og ved endelig registrering. Herudover skal sagsbehandlere kunne tilføje tekster ved manuel behandling.

5.17.7 Tillægstekster

Tillægstekster er et begreb, som findes i det nuværende system. De benyttes bl.a. til at indikere at noget er lyst på flere objekter. Hvis et pantebrev eksempelvis er lyst på flere ejendomme, vil pantebrevet optræde som hæftelse på de enkelte ejendomme sammen med en tillægstekst, som siger ”Tillige lyst på ...”. Den funktion, som tillægstekster har haft i det eksisterende system vil i de fleste tilfælde kunne automatiseres fremover, men skal også kunne tilføjes af sagsbehandlere ved manuel behandling. Konceptuelt er der ingen forskel på standardtekster og tillægstekster, hvorfor disse to begreber bør slås sammen i det nye tinglysningsystem..

5.17.8 Opdatering

For alle typer af fraser gælder det, at det ikke er muligt at ændre disse, når de først har været anvendt én gang. Det skal dog være muligt at markere at en frase ikke kan bruges efter en bestemt

- `identifikation` – en kort og sigende identifikationstekst, typisk et eller få ord. Den har samme anvendelse som kode, men ved anmeldelser i XML strukturen for tinglysningsdokumentet skal anmelder benytte `identifikation` i stedet og ikke kode
- `tekst` – den konkrete tekst for frasen. Teksten kan indeholde reference til de felter, som frasen har, således at værdierne for felterne kan flettes med frasen til en sammenhængende tekst. Det antages for nuværende at frasen kan formuleres så der ikke opstår problemer omkring entals- og flertalsformer. Angivelsen af hvor et felt skal flettes ind vil være på formen `@{FeltNavn}`.
- `gyldigFra` – første dag hvor frasen kan anvendes (uden tidspunkt)
- `gyldigTil` – sidste dag, hvor frasen kan anvendes (uden tidspunkt)
- `ekspeditionstyper` – relation til de ekspeditionstyper, hvor frasen er relevant. Der indføres også en kategorisering/gruppering af fraser, så det er muligt at referere en samling af ekspeditionstyper.
- `fraseFelter` – relation til beskrivelse af de felter, som frasen indeholder
- `gruppe` – relation til den gruppe som frasen er en del af. Grupper repræsenteres af `FraseGruppe`, som beskriver gruppen. For vilkår kan dette benyttes til at danne de forskellige vilkårsmoduler
- `fuldmagtsdefinition` – hvis der er tale om en fuldmagtstekst vil der være en relation til en `Fuldmagtsdefinition`, som beskriver hvilken fuldmagt der skal oprettes

Klasserne `FraseFelt` og `FraseFeltVærdi` specificerer de variable felter, som indgår i frasen. `FraseFelt` har følgende informationer.

- `type` – angiver typen af feltet. De mulige typer er defineret i enumerationen `FraseFeltType`
- `navn` – navn på feltet
- `beskrivelse` – beskrivelse af den information som feltet indeholder
- `fraseFeltVærdi` – relation til et antal `FraseFeltVærdi`, som er den liste af værdier, som kan benyttes. Det er kun hvis `type` er `STRING_LISTE_FAST` eller `STRING_LISTE_ÅBEN` at denne relation benyttes

Hvis frasen er en erklæring (feltet `type` i `Frase` har værdien `ERKLÆRING`), så kan der være flere egenskaber ved frasen. Dette er udtrykt ved nedarvning til `Erklæring`. `Erklæring` indeholder følgende information.

- `anvendelse` – angiver hvilken type af anvendelse erklæringen har. Enumerationen `ErklæringAnvendelse` indeholder de mulige værdier
- `erklæringsKriterier` – angiver kriterier for under hvilke omstændigheder erklæringen skal afgives. Enumerationen `ErklæringKriterieType` indeholder de mulige kriterier. Fx angiver `KØBER_CVR`, at erklæringen skal afgives hvis køber på et skøde er en virksomhed
- `erklæringsUnderskrifter` – relation til et antal `ErklæringsUnderskrift`, som angiver de roller som skal underskrive tinglysningsdokumentet hvis erklæringen er afgivet. Værdier i denne relation er kun nødvendige hvis erklæringen kræver flere underskrifter end de normale dispositionsrettigheder bestemmer
- `kendt` – angiver, at det er tale om en "kendt" erklæring. Det betyder at der er tale om en erklæring, som kontrollerer i den automatiske prøvelse skal kunne forstå og behandle. Klassen `KendtErklæring` beskriver de kendte erklæringer, som systemet kan behandle. Hver `KendtErklæring` vil have en kode, som kan benyttes af kontrollerne til at checke for en given kendt erklæring. En erklæring, som ikke er relateret til en "kendt" erklæring vil ikke kunne udsættes for automatisk prøvelse.
- `forudsætning` – relation til en anden erklæring, som er en forudsætning for at erklæringen kan angives. Hvis den erklæring, som forudsætning ikke er afgivet kan den aktuelle erklæring heller ikke afgives

- modstridende – relation til en andre erklæringer, som er modstridende med erklæringen. Hvis en eller flere af de modstridende erklæringer er afgivet kan den aktuelle erklæring ikke afgives

Uafklaret: Vil anvendelsen for en erklæring være generel, eller vil den være afhængig af ekspeditionstypen? Hvis den kan være afhængig af ekspeditionstypen, så dette også kunne angives.
Afklaret: Det er allerede dækket af relationen ekspeditionstyper på Frase.

Uafklaret: Giver det nogen mening at gyldigFra og gyldigTil indeholder tidspunkt.
Afklaret: gyldigFra og gyldigTil vil kun indeholde dato og ikke tid, det er også det som står ovenfor.

Bemærkning: Måske skal Frase også nedarves til Fuldmagt, da relationen fuldmagtsdefinition kun er relevant for fuldmagter,