



e-TL System til System grænseflader

Version	Dato	Forfatter	Kommentarer	Distribueret til
0.9	10/10-07	Tommy D. Pedersen	Første udkast	Test og Teknikgruppen, DSS og Devoteam



Indholdsfortegnelse

Formål.....	3
Anmeldelsesscenarie til meddelelsestest.....	4
RASP - Anmeld.....	7
S2S-register.....	9
Administrationscertifikater.....	10
Transportcertifikater.....	10
Anmeldercertifikater.....	11
Kommunikationskanal til svar.....	12
Integration.....	13
RASP for Java.....	13
Eksempel på en RASP klient.....	14
Fejlliste.....	15
Udeståender.....	15



e-TL System til System snitflader

Formål

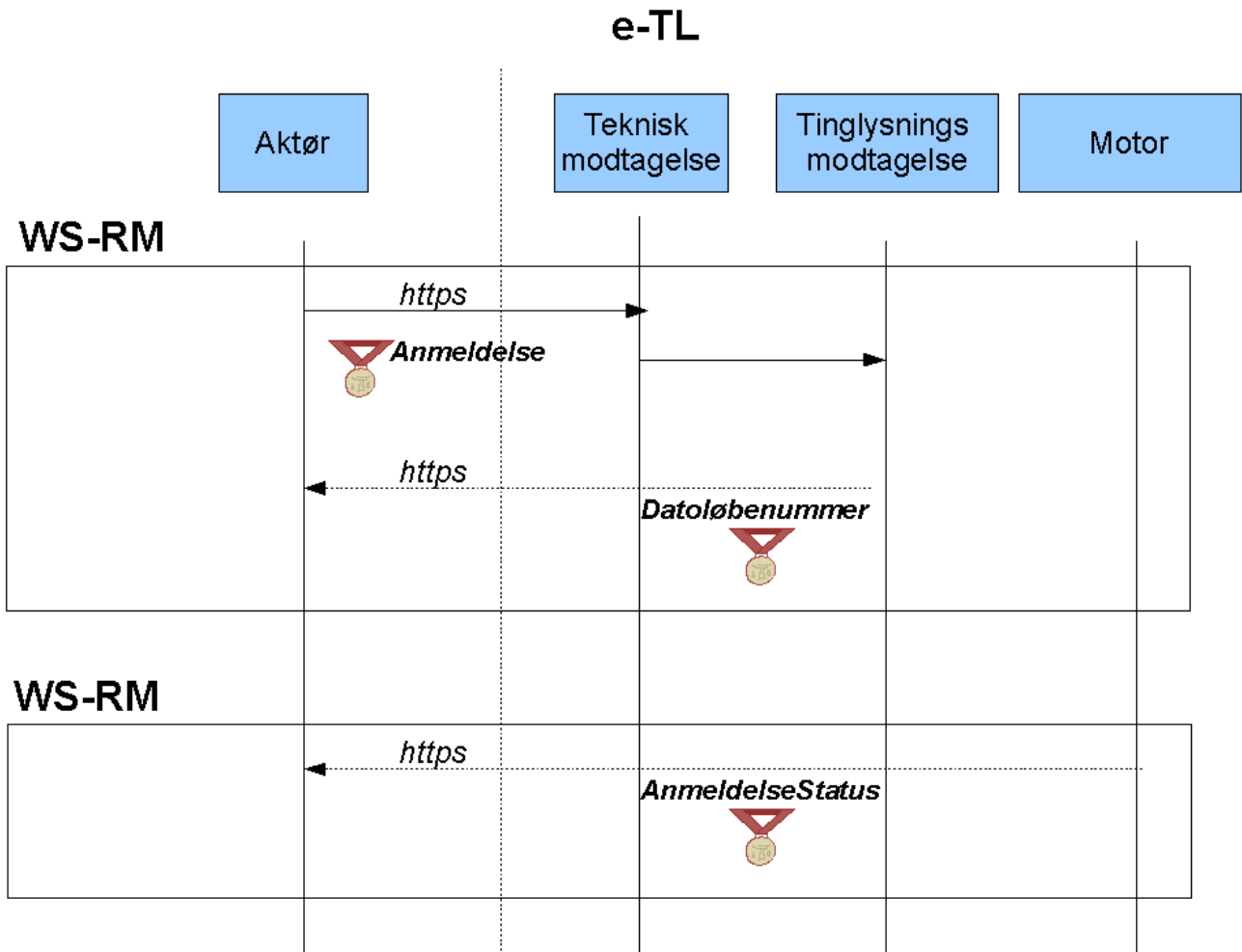
Dette dokument har til formål at præcisere deltagerne i den servicesnitflade e-TL stiller til rådighed for de eksterne system-til-system brugere.

Dokumentet skal ses i sammenhæng med løsningsbeskrivelsens afsnit 4 fra 1. juni 2007.

Ved forskelle i de 2 dokumenter vil det være dette dokumentets indhold der er gældende.

Anmeldelsesscenarie til meddelelsestest

Alle anmeldelser og statussvar sendes til og fra e-TL som selvstændige RASP-beskeder; det drejer sig om den initierende "anmeld"-besked, og de efterfølgende statusbeskeder.





e-TL System til System snitflader

Herunder listes eksempler på RASP-beskeder; bemærk, beskeder med nummer 2 og derover ikke er endeligt fastlagt og derfor blot er foreløbig indikation.

Aktør	eTL
[1. Anmeld <-> Datoløbenummer]	
	[2a. Afvisning ved modtagelse]
	[2b. Estimeret behandlingstid]
	[3. Manuel behandling + estimeret behandlingstid]
	[4a. Afvist i sagsbehandling]
	[4b. Tinglyst]
	[4c. Tinglyst med frist]

1. Anmeld

Når en "anmeld"-besked er leveret, er Aktør garanteret, at eTL har modtaget anmeldelsen, at anmeldelsen er tildelt datoløbenummer og sat i kø til sagsbehandling. Aktør skal annotere beskeden med et Aktør-unikt besked-id (ifølge RASP via SOAP Custom Header). Dette id benyttes til at sikre *exactly-once*. I svaret leveres datoløbenummer.

Hvis transportcertifikat ikke er registreret hos eTL, svares tilbage med vejledende SOAP-fejl.

2a Afvisning ved modtagelse

Aktør notificeres om, at anmeldelsen er afvist ved modtagelse. Årsager kan eksempelvis være ukendt anmeldercertifikat, ugyldigt xml eller mangler i anmeldelse. Svaret annoteres med datoløbenummer.

Denne besked markerer en sluttilstand.



2b Estimeret behandlingstid

Aktør notificeres om, at anmeldelsen er klar til sagsbehandling, om anmeldelsen er blokeret af andre sager, og estimeret behandlingstid. Svaret annoteres med datoløbenummer.

3 Manuel behandling + estimeret behandlingstid

Det er under sagsbehandlingen konstateret, at manuel sagsbehandling er påkrævet, samt ny estimeret behandlingstid. Beskeden er optionel, og kan kun følge efter 2b.

4a-c

De forskellige mulige sluttilstande for tillysningsforløbet.



RASP - Anmeld

I RASP-regi garanterer eTL *exactly-once*, dvs. hvis den samme "anmeld"-besked sendes mere end én gang, returneres svaret, som blev returneret til den oprindelige "anmeld"-besked. Helt præcist returneres det datoløbenummer, anmeldelsen tidligere har fået tildelt.

Det skal bemærkes, at selv om "anmeld"-beskeden fejler, kan anmeldelsen godt være tildelt datoløbenummer og sat i kø til sagsbehandling, for detaljer se detaljeret gennemgang af RASP-session nedenunder. Men Aktør kan blot sende beskeden igen, og eTL opdager at anmeldelsen er modtaget tidligere, og giver det samme svar som tidligere returneret (datoløbenummer).

Hvis "anmeld"-beskeden fejler, men anmeldelsen er tildelt datoløbenummer i eTL, kan det resultere i scenariet, at Aktør modtager statusbeskeder, mens Aktør er ved at gensende "anmeld"-beskeden:

1. Aktør sender "anmeld"-besked. [1. Anmeld]
2. eTL tildeler anmeldelse datoløbenummer og registrerer modtagelse. Herefter kan eTL notificere Aktør med statusbeskeder, selv om resten af RASP-sessionen fejler.
3. Kommunikationen mellem Aktør og eTL fejler, og "anmeld"-beskeden fejler på Aktør-siden, dvs Aktør modtager en fejlbesked fra RASP, og har endnu ikke modtaget datoløbenummer.
4. eTL melder asynkront tilbage om påbegyndt sagsbehandling på et datoløbenummer, som Aktør endnu ikke kender. [2b. Estimeret behandlingstid]
5. Ifølge RASP-specifikationen forsøger Aktør at sende den samme besked igen (gensendelse). [1. Anmeld]
6. eTL genkender, at Aktør har sendt den samme besked igen, og svarer tilbage med det oprindelige datoløbenummer. [1. Anmeld]
7. Aktør får nu svar tilbage fra gensendelse, inkl datoløbenummer. Aktør kan nu knytte de allerede modtagne notifikationer sammen med oprindelig anmeldelse.



e-TL System til System snitflader

Detaljeret gennemgang af RASP-session

Her vises kort, hvorledes en RASP-session forløber ved en anmeldelse, specielt hvornår man kan forvente at anmeldelsen er tildelt datoløbenummer og transaktionelt udført. Når anmeldelsen er tildelt datoløbenummer starter sagsbehandlingen.

```
Aktør                eTL

    == Create sequence =====>

<== Ack =====

    == Body (anmeldelse) ===>

                                Datoløbenummer tildelt

<== Datoløbenummer =====

    == Last message =====>

<== Ack =====

    == Terminate sequence ==>

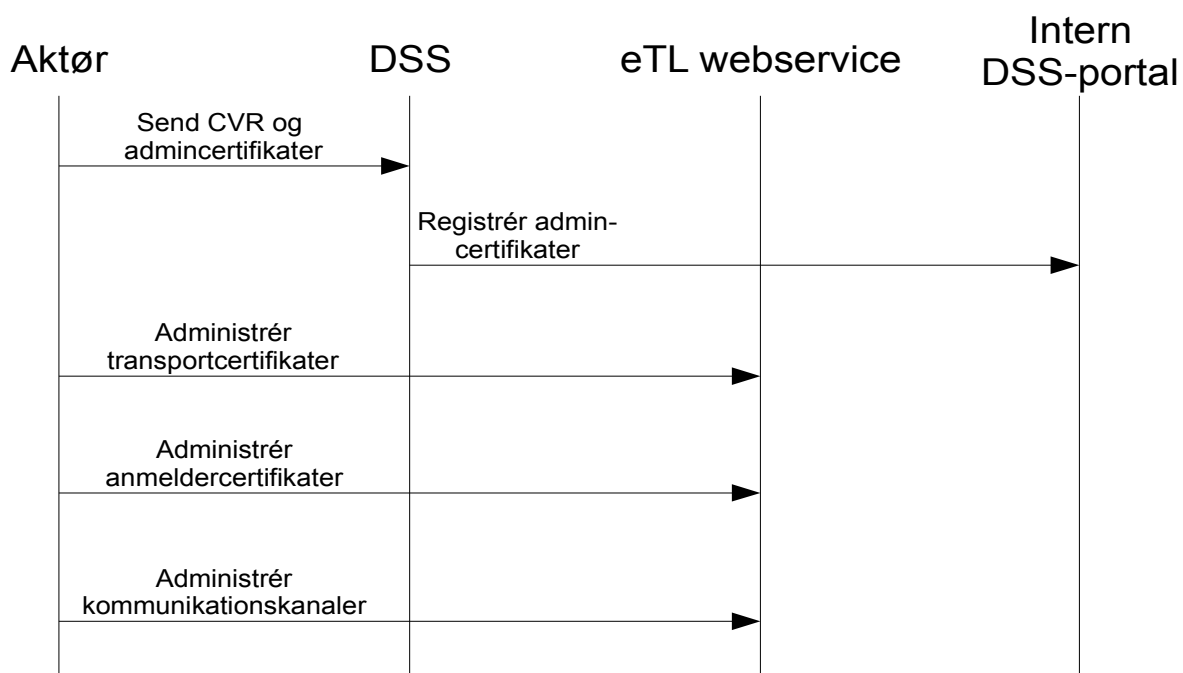
<== Ack =====
```



S2S-register

Her listes objekter, som skal registreres pr S2S-aftale. Det er endnu uvist om en Aktør kan have flere S2S-aftaler.

Processen med at registrere, og efterfølgende administrere, en Aktør i eTL kan skitseres således:



Registeret skal indeholde nedenstående oplysninger om Aktørs eksterne system.

Navn	Note
<i>CVR-nr</i>	
<i>Administrations-certifikater</i>	Certifikat benyttes til at administrere Aktørs certifikater og kommunikationskanaler. Se specifikation nedenunder.
<i>Transportcertifikater</i>	Certifikater benyttet til transport. Se specifikation nedenunder.
<i>Anmeldercertifikater</i>	Certifikat benyttet til signering af anmeldelser. Se specifikation nedenunder.
<i>Kommunikationskanal til svar</i>	Webservice-endpoints, som kan modtage svar fra eTL. Se specifikation nedenunder.



Administrationscertifikater

Certifikater i denne kategori skal benyttes når en virksomhed ønsker at administrere virksomhedens andre certifikater, såsom sine transportcertifikater. Registrering af administrationscertifikaterne er en opstartsproces, der skal være udført for at Aktør teknisk kan benytte sig af System-til-system-ordningen.

Navn	Note
<i>Teknisk administrations-certifikat</i>	Dette certifikat skal signere webservice-forespørgsler, som kan ændre virksomhedens transportcertifikater. Certifikatet skal kunne benyttes til signering. Certifikatet kan kun opdateres af DSS gennem intern portal.
<i>Anmelder-administrations-certifikater</i>	Dette certifikat skal signere webservice-forespørgsler, som kan ændre virksomhedens anmelder- og disponentcertifikater. Certifikatet skal kunne benyttes til signering. Certifikatet kan kun opdateres af DSS gennem intern portal.

Transportcertifikater

Disse certifikater benyttes når beskeder transporteres mellem Aktør til eTL.

Navn	Note
<i>RASP-certifikat</i>	Benyttes af Aktør når en forespørgselsbesked signeres. Benyttes af eTL når en svarbesked signeres. Certifikatet skal kunne benyttes til signering. Vil oftest være et OCES-device-certifikat. Kan være gennemstillingssystemets certifikat, f.eks. EFPI's certifikat. Kan opdateres via webservice med Teknisk administrationscertifikat.
<i>SSL-servercertifikat</i>	Benyttes af eTL når en svarbesked skal afleveres til Aktør. Certifikatet skal kunne benyttes til at kryptere kommunikationen med Aktør. Kan være gennemstillingssystemets certifikat, f.eks. EFPI's certifikat. Kan opdateres via webservice med Teknisk administrationscertifikat.



Anmeldercertifikater

Disse certifikater benyttes til at signere en anmeldelse, dvs. indholdet af en RASP-besked.

Disse oplysninger er kompileret fra *e-TL_Bilag_2_Kravspecifikation.doc*, afsnit 6.18.

Navn	Note
<i>Medarbejdercertifikat</i>	Benyttes af medarbejder hos Aktør når en anmeldelse signeres. Certifikatet skal kunne benyttes til signering. Kan opdateres via webservice med Anmelder-administrationscertifikat.
<i>Virksomhedscertifikat</i>	Benyttes af en Aktørs system til at signere anmeldelser Certifikatet skal kunne benyttes til signering. Kan opdateres via webservice med Anmelder-administrationscertifikat. Et virksomhedscertifikat kan have begrænsninger i lovlige anmeldelser (se <i>e-TL_Bilag_2_Kravspecifikation.doc</i> , afsnit 6.18.2). Disse begrænsninger kan opdateres via webservice med Anmelder-administrationscertifikat.
<i>Tegningscertifikat</i>	Benyttes til at signere hæftelser og pantsætninger på vegne af Aktør. Kan tildeles til medarbejdere hos Aktør. Certifikatet skal kunne benyttes til signering. Kan opdateres via webservice med Anmelder-administrationscertifikat. Certifikatet registreres i underskriftsdata-basen, se <i>e-TL_Bilag_2_Kravspecifikation.doc</i> , afsnit 6.19.2.1.



Kommunikationskanal til svar

Kommunikationskanalen er det webservice-endpoint, som eTL sender svar tilbage til Aktør på.

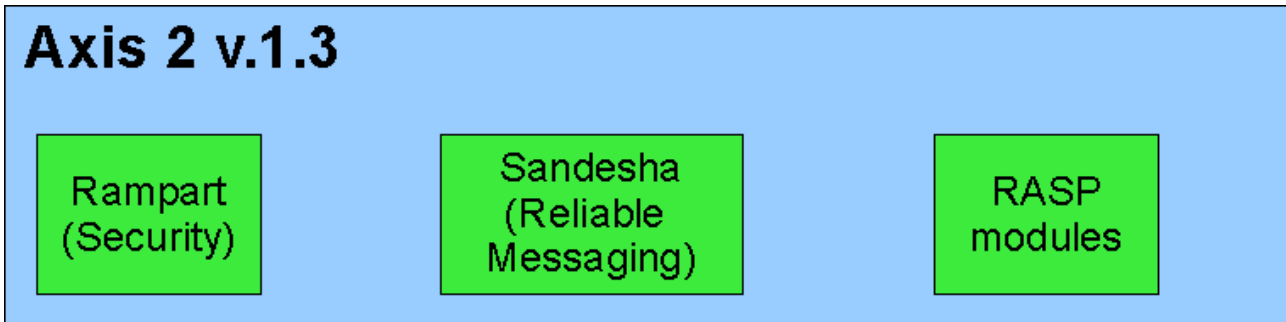
Følgende skal registreres for et endpoint.

Navn	Note
<i>Endpoint</i>	RASP-beskeder sendes tilbage til dette endpoint.
<i>SSL-servercertifikat</i>	Et SSL-servercertifikat, som er registreret under Transportcertifikater. RASP-svarbeskeder krypteres mellem Aktørs server og eTL med dette certifikat.

Oplysningerne kan opdateres via webservice med Teknisk administrationscertifikat.

Integration

RASP for Java



Overordnet set er RASP for Java

- en pre-konfigureret Apache Axis 2 v. 1.3
- en komponent til afvikling på forskellige Java applikations servere herunder Tomcat, Jboss og BEA.
- RASP indeholder standard Apache moduler til håndtering af XML security (Rampart) og reliability (Sandesha).
- Custom RASP moduler implementerer logging, validering, certifikathåndtering, UDDI opslag og signaturbevis.
- RASP API til enkel programmering af klienter og services.
- Egne moduler kan udvikles og indbygges.





Eksempel på en RASP klient

```
OiosiMessage oiosiMessage = new OiosiMessage( xmlDoc );

oiosiMessage.setRequestAction(
    documentTypeConfig.getEndpointType().getRequestAction() );

oiosiMessage.setReplyAction(
    documentTypeConfig.getEndpointType().getReplyAction() );

KeyStore ks = KeyStore.getInstance( "JKS" ).load()...

X509Certificate server =
    (X509Certificate) ks.getCertificate( "server" );

Credentials credentials =
    new Credentials( new OcesX509Certificate( server ) );

Request request =
    new Request(endpointAddress, credentials, sendPolicy );

Response response = request.getResponse( oiosiMessage );
```



Fejlliste

Fejl i RASP kommunikation overholder principper i løsnings-specifikationens afsnit 4.2.3.3.

Her kommer en liste over generelle RASP fejl – service-specifikke fejl fremgår senere i relation til specifikke services.

Udeståender

Præcisering af sammenhæng mellem roller og signaturer

XML Schema for Anmeldelse (TLS_Anmeldelse.xsd) tillader ikke brug af ID attribut på Anmeldelse.