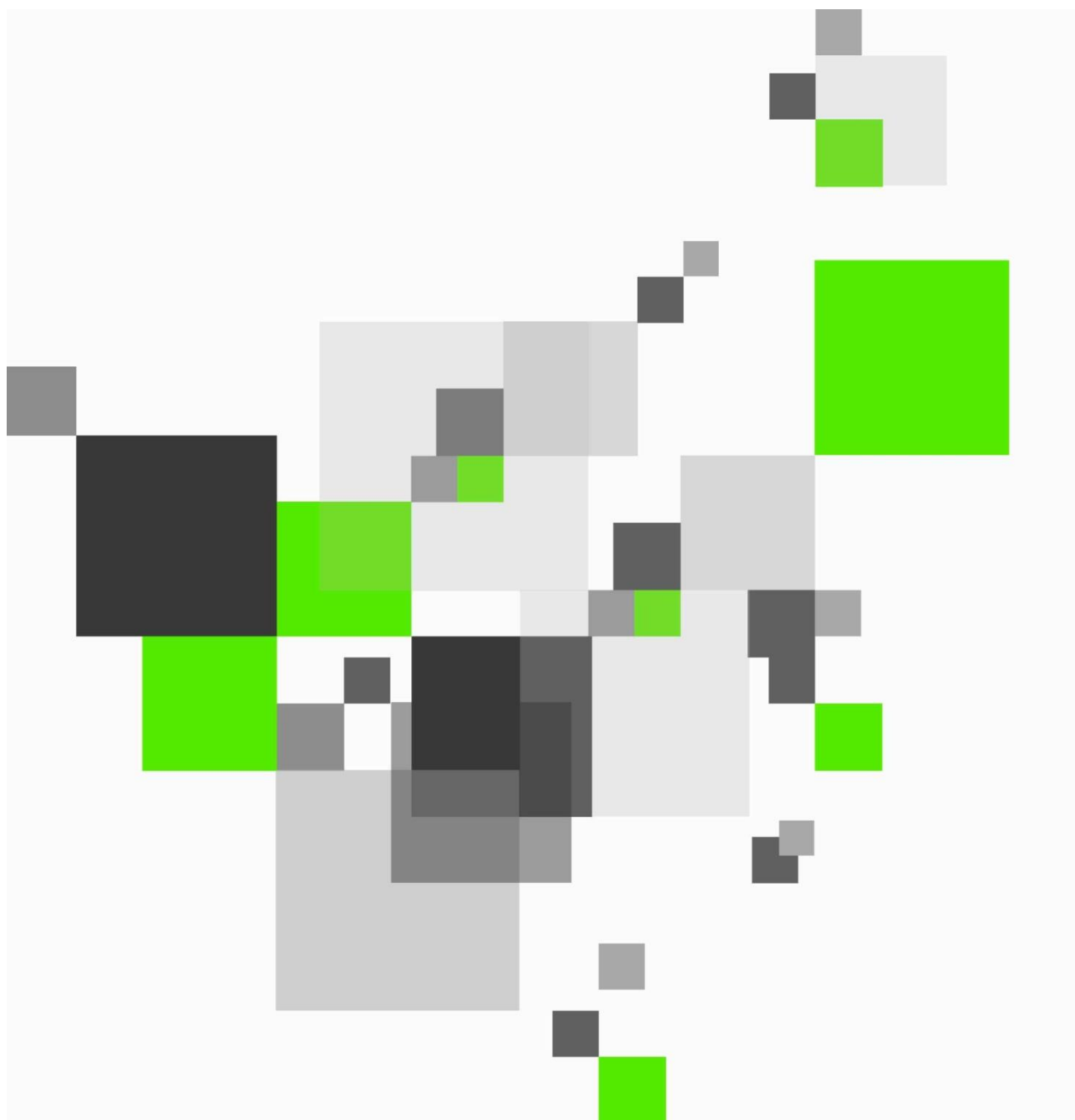


Besked-Aflever-Snitflade



Indholdsfortegnelse

Historik	3
1. Versioner	<u>54</u>
2. Målgruppe	<u>54</u>
3. Snitfladebeskrivelse for SF1460_A	<u>54</u>
4. Servicebeskrivelse	<u>65</u>
5. Funktionalitet i operationen Aflever Besked	<u>65</u>
5.1. Inputdokument.....	<u>65</u>
5.2. Outputdokument	<u>76</u>
6. Teknisk beskrivelse	<u>87</u>
6.1. Sikkerhed	<u>87</u>
6.2. SecurityPolicy	<u>87</u>
6.3. Certifikater	<u>87</u>
6.4. Autorisation	<u>87</u>
6.5. Skemavalidering	<u>98</u>
7. Kommunikation	<u>98</u>
7.1. Håndtering af utilgængelighed i snitfladen	<u>98</u>
7.2. Angivelse af transaktionsId i snitfladen	<u>109</u>
8. Transformationsmekanismer	<u>109</u>
9. Eventuelt yderligere oplysninger	<u>109</u>
10. Bilag 1 trustede certifikatudstedere for endpoint SSL	<u>1110</u>
11. Appendiks 1 – eksempler.....	<u>1514</u>
11.1. Inputstruktur - Besked Aflever	<u>1514</u>
11.2. Outputstruktur - Besked Aflever	<u>1716</u>
12. Appendiks 2 – Fejlsøgning	<u>1817</u>
13. Appendiks 3 – serviceaftale og dataafgrænsning.....	<u>2018</u>

Historik

Dato	Dokumentversion	Revideret af	Ændring	BF version
2016-09-09		MSG	Oprettet revisionshistorik. Præciseret versionsnummer af snitflade og -beskrivelse.	1.4.7
2016-10-18		MMM	Opdateret Beskedfordeler.wadl til Anvendelsesystem.wadl afs. 4.1 Angivet at modtagersystemets service certifikat skal være identisk med det certifikat der er registreret for servicen i Støttesystemernes administrationsmodul Diverse sproglige om formuleringer	1.4.7
2017-09-15	2.0	BIW	Mulighed for at registrer selvstændige certifikater til endpoints og anvende SSL certifikat i servicen Tilføjet liste over trusted SSL certifikat udstedere for endpoint certifikater.	2.0
2017-12-11	3.0	BIW	Service navn i kapitel 3 ændret, fra " Modtag besked " til " Modtagbesked "	2.0
2018-06-13	4.0	BIW	Ej frigivet	2.0
2018-06-13	5.0	BIW	Eksempler på strukturer tilføjet Eksempler på fejlsituationer tilføjet Illustration af snitflader tilføjet	2.0
2020-01-14	6.0	BIW	Retursvar i eksempel opdateret i afsnit 11.2 SecurityPolicy indsat fra fællesdokumentet + appendiks 3 med dataafgrænsninger indsat	2.0
2022-03-16	7.0	MSG	Ændring af format i Ansvarlig Myndighed i Appendiks 3 jf. SRITM0870030	2.0

1. Versioner

Snitfladebeskrivelsens version er: Version 6.0

Snitfladens version er 1.0.0

- Service specifikation: Anvendersistem.wadl

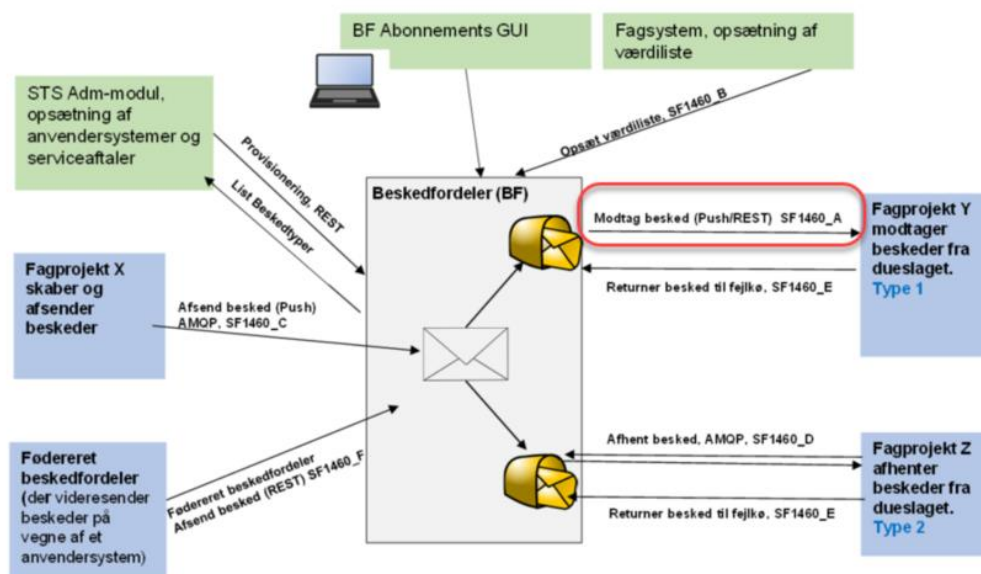
2. Målgruppe

Integrationsudviklere der arbejder hjemmefrem med SOAP og REST teknologier.

3. Snitfladebeskrivelse for SF1460_A

Nærværende dokument beskriver, hvorledes en service, **Aflever Besked**, skal konstrueres af **Modtagersystemet** for at kunne få leveret beskeder fra **Beskedfordeler**.

Beskeder kan afleveres til **Modtagersystemer** fra deres dueslag i **Beskedfordeler**, hvis dette er angivet på dueslaget i **Beskedfordeler**s brugergrænseflade. **Modtagersystemets** endpoint (URL) angives i **Administrationsmodulet**, som et callback endpoint konfigureret for **Modtagersystemet**.



Figur 1: Beskedfordelerens grænseflader. AfleverBesked-Snitflade er markeret med rød firkant

Vilkårene for at integrere til **Beskedfordeler** er beskrevet i Underbilag 2N: Vilkår for integration til **Beskedfordeler**. Attributter, der indgår i operationerne, er nærmere beskrevet i informationsmodel og specifikation for **Beskedkuvert** i underbilag 2O. Link til dokumenterne findes i afsnit 9.

4. Servicebeskrivelse

For at **Beskedfordeler** kan aflevere beskeder til **Anvendersystemerne**, skal de implementere denne REST web service. I **Anvendersystemernes** snitfladebeskrivelser, kaldes denne service for **Modtagbesked**.

Snitfladen skal kunne modtage en besked af typen **Haendelsesbesked**, som er opbygget af **Beskedversion**, **Beskedkuvert** og **Beskeddata**. **Beskedkuvert** entiteten struktureres som beskrevet under yderligere oplysninger, underbilag 20 - Beskedkuvert. **Beskedversion** samt **Beskedkuvert** er en tekstuel streng, og **Beskeddata** kan være i en struktur, der afspejler det enkelte objekt, som beskeden omhandler.

Det er et krav til **Modtagersystemet**, at det skal kunne håndtere at modtage den samme besked med samme **Haendelsesbesked.BeskedId** flere gange uden at fejle.

5. Funktionalitet i operationen Aflever Besked

Snitfladen er en beskrivelse af det REST endpoint hos **Modtagersystemet**, som muliggør at få leveret beskeder fra det fælleskommunale støttesystem **Beskedfordeler**. Snitfladen skal kunne modtage et **HaendelsesBesked** objekt ud fra **Beskedfordelers** input. Snitfladen skal kunne håndtere at modtage samme besked flere gange.

Når beskeder havner i et dueslag, som endpointet er tilknyttet, kalder **Beskedfordeler** servicen og forsøger at aflevere beskeder fra dueslaget. Beskeder afleveres i samme rækkefølge, som de er distribueret til dueslaget. **Beskedfordeler** afleverer kun beskeder fra dueslag, der er markeret som aktiv i **Beskedfordelers** brugergrænseflade.

5.1.Inputdokument

Nedenstående skal kunne modtages af REST snitfladen hos Anvendersystemet. (se Beskedfordelerens kodeeksempler).

I "~~Appendiks 1 - eksempler~~[Appendiks 1 - eksempler](#)" afsnit "11.1 ~~Inputstruktur - Besked Aflever~~[Inputstruktur - Besked Aflever](#)" er der eksempel på, hvordan inputstrukturen kan se ud.

Struktur	Beskrivelse
ModtagBeskedInput	<p>XML dokumentet overholder det tilhørende skema, som angiver struktur og ved attributter hvilke, der er obligatoriske. Se Anvendersystem.wadl</p> <p>Beskeder overholder det tilhørende skema (Beskedkuvert.xsd), som angiver syntaksen for Beskedhændelser her under Beskedkuvertversion.</p>

5.2. Outputdokument

REST servicen skal returnere et XML dokument, som består af en standard retur struktur.

I "~~Appendiks 1 – eksempler~~Appendiks 1 – eksempler" afsnit "11.2 Outputstruktur - Besked Aflever" er der eksempler på, hvordan outputstrukturen kan se ud. I "~~Appendiks 2 – Fejlsøgning~~Appendiks 2 – Fejlsøgning" er der forslag til fejlsøgning, hvis beskeder ikke modtages som forventet.

Struktur	StatusKode	Fejlbesked
ModtagBeskedOutput der indeholder en StandardRetur	20	Ok
	40	Besked kan ikke modtages
	51	Service ikke implementeret
	53	Service ikke tilgængelig
	55	Service version ikke understøttet

Når **Anvendersystemet** giver status 20 – OK tilbage, anses beskeden for overdraget til **Modtagersystemet**, og beskeden fjernes fra dueslaget.

Ved angivelse af status 40 afbrydes afleveringen til **Modtagersystemet** midlertidigt, og beskeden forbliver på køen. Ved øvrige fejl stoppes afsendelsen af beskeder fra dueslaget. Beskeden betragtes kun som overdraget, hvis der modtages en http statuskode 20. Alle andre http statuskoder end 20 resulterer i, at beskeden forbliver på dueslaget og beskeden bliver efter en forsinkelse forsøgt genleveret, indtil beskeden kan leveres eller dueslaget markeres inaktivt.

6. Teknisk beskrivelse

Servicen skal implementeres som en REST web service.

6.1.Sikkerhed

Servicen skal sikres med 2-vejs SSL via

- **Beskedfordelers** system certifikat, der er velkendt, samt
- **Modtagersystemets** certifikat til etablering af TLS version 1.2 forbindelsen. Endpoint serveren skal understøtte Beskedfordeler's certifikat fulde trust chain, der medsendes ved etablering af forbindelse.

Forudsætninger for at kunne oprette 2-vejs SSL er:

- at endpointet hos modtagersystemet truster Beskedfordelerens FOCES certifikat. Certifikatet er unikt pr. miljø.
- at Beskedfordeleren truster endpoint serverens servercertifikat. For at det sker skal certifikatet ved udstedt af en af leverandørerne fra "Bilag 1 trusted certifikatudstedere for endpoint SSL" Der kan benytte FOCES eller SSL certifikater til at beskytte endpointet.
- at fra version 2.0.1 af Beskedfordeler skal nye endpoint certifikater være SSL certifikater.

Efter at 2-vejs SSL er etableret verificeres at modtagersystemets udstillede Certifikat er identisk med det certifikat der registreres til servicen endpoint i Støttesystemernes Administrationsmodul. Det sker for at sikre, at endpoint er ejet af samme modtagersystem som ejer Dueslaget, hvorfra beskeder sendes.

6.2.SecurityPolicy

Der anvendes i Beskedfordeleren's snitflader en blanding af Tokensikkerhed og certifikatsikkerhed. Denne service er af type "**Simple callback service**", hvor Servicen autentificerer anvendelsesystemet via et SSL/TLS-klientcertifikat, der registres i Administrationsmodulet.

6.3.Certifikater

Beskedfordeler identificeres i **Modtagersystemet** via det medsendte anvender-certifikat, som er et FOCES 2 funktionscertifikat. Modtagersystemets endpoint kan beskyttes med enten FOCES eller SSL certifikat. Endpointets certifikatet indgår først i etableringen af en SSL forbindelse. Dvs at beskedfordeler truster certifikatet i forhold til listen (appendiks 1). dernæst matches certifikatet mod den provisionerede certifikat til endpointet for at sikre en trusted forbindelse til det Dueslag, der afleveres beskeder fra.

6.4.Autorisation

Beskedfordeler autoriseres til at kalde snitfladen ved, at **Beskedfordelers** certifikat er velkendt af **Modtagersystemet**. Mulighederne for dataafgrænsninger gældende for

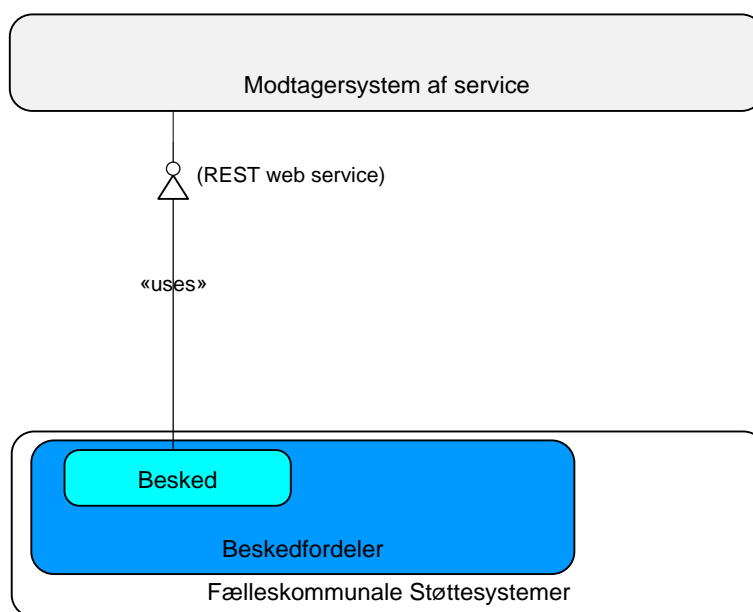
abonnementer der kan filtrere de beskeder der kan hentes via snitfladen er beskrevet i Appendiks 3 – serviceaftale og dataafgrænsning

6.5. Skemavalidering

Ved modtagelse af beskeder skal Anvendersystemet foretage en skemavalidering af Beskedens XML for overholdelse af bl.a. version, format og gyldighed af tags i henhold til den givne operation.

7. Kommunikation

Snitfladen er et synkron web-service kald, der udføres direkte ved kald fra det fælleskommunale støttesystem **Beskedfordeler** til **Modtagersystemet**.



*Figur 1 Kaldet til Besked-Aflever-snitfladen er et synkron web service kald, som udføres direkte til **Modtagersystemet** fra **Beskedfordeler**.*

7.1. Håndtering af utilgængelighed i snitfladen

Servicen skal sikres mod nedbrud. Som for alle synkrone opdaterede services vil det kunne ske ved, at beskeden afsendes, uden at **Beskedfordeler** modtager et svar fra **Modtagersystemet**. Det kan feks. skyldes netværksfejl. Hvis **Beskedfordeler** ikke modtager svar, forbliver beskeden i dueslaget og vil efterfølgende blive forsøgt afleveret igen. Beskeden forsøges afleveret af Beskedfordeleren med længere og længere intervaller indtil at den kan modtages af servicen.

Servicen skal være idempotent med hensyn til, at **Modtagersystemet** skal kunne modtage den samme besked med samme unikke Haendelsesbesked.BeskedId iht. **Beskedkuverten**, flere gange.

7.2. Angivelse af transaktionsId i snitfladen

Beskedkuverten indeholder flere ID'er der identificerer forskellige dele af den komplekse hændelse som beskeden udgør. Ved generering af beskeden vil det transaktionsgenererende system, Afsendersystemet udfylde "Haendelsesbesked.BeskedId" som udgør et Transaktions ID fra afsender til modtager. Beskedfordeler påsætter ved modtagelsen af beskeden der ud over et "Leveranceinformation.TransaktionsId" på beskedkuverten.

Et Modtagersystem kan således altid være sikker på at en besked er unik. Modtagersystemet kan via Haendelsesbesked.BeskedId registrere den samlede transaktion for beskeden. Modtagersystemet kan også via Leveranceinformation.TransaktionsId registrere transaktionen for aflevering af beskeden.

8. Transformationsmekanismer

N/A

9. Eventuelt yderligere oplysninger

Links til Beskedkuvert skemaer, endpoints og anden dokumentation vedr. snitfladerne finder du via siden: https://share-komm.kombit.dk/P133/_layouts/15/start.aspx#/ Fra siden "Service- og ydelseskataloger" vælger du oversigtslinket "referencedokumenter".

10. Bilag 1 trustede certifikatudstedere for endpoint SSL

Owner	Certificate Issuer Organization	Certificate Issuer Organizational Unit	Common Name or Certificate Name
Comodo	Comodo CA Limited		AAA Certificate Services
Comodo	AddTrust AB	AddTrust TTP Network	AddTrust Class 1 CA Root
Comodo	AddTrust AB	AddTrust External TTP Network	AddTrust External CA Root
Comodo	AddTrust AB	AddTrust TTP Network	AddTrust Public CA Root
Comodo	AddTrust AB	AddTrust TTP Network	AddTrust Qualified CA Root
Comodo	COMODO CA Limited		COMODO Certification Authority
Comodo	COMODO CA Limited		COMODO ECC Certification Authority
Comodo	COMODO CA Limited		COMODO RSA Certification Authority
Comodo	Comodo CA Limited		Secure Certificate Services
Comodo	Comodo CA Limited		Trusted Certificate Services
Comodo	The USERTRUST Network		USERTrust ECC Certification Authority
Comodo	The USERTRUST Network		USERTrust RSA Certification Authority
Comodo	The USERTRUST Network	http://www.usertrust.com/	UTN-USERFirst-Client Authentication and Email
Comodo	The USERTRUST Network	http://www.usertrust.com/	UTN-USERFirst-Hardware
Comodo	The USERTRUST Network	http://www.usertrust.com/	UTN-USERFirst-Object
DanID	Nets DanID A/S		Rodcertifikat TRUST2408 OCES Primary CA
DigiCert	Baltimore	CyberTrust	Baltimore CyberTrust Root
DigiCert	Cybertrust, Inc		Cybertrust Global Root
DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert Assured ID Root CA
DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert Assured ID Root G2
DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert Assured ID Root G3

DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert Global Root CA
DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert Global Root G2
DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert Global Root G3
DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert High Assurance EV Root CA
DigiCert	DigiCert Inc	http://www.digicert.com/	DigiCert Trusted Root G4
Entrust	AffirmTrust		AffirmTrust Commercial
Entrust	AffirmTrust		AffirmTrust Networking
Entrust	AffirmTrust		AffirmTrust Premium
Entrust	AffirmTrust		AffirmTrust Premium ECC
Entrust	Entrust, Inc.	www.entrust.net/CPS is incorporated by reference	Entrust Root Certification Authority
Entrust	Entrust, Inc.	See www.entrust.net/legal-terms	Entrust Root Certification Authority - EC1
Entrust	Entrust, Inc.	See www.entrust.net/legal-terms	Entrust Root Certification Authority - G2
Entrust	Entrust.net	www.entrust.net/CPS 2048 in-corp. by ref. (limits liab.)	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign	GlobalSign ECC Root CA - R5	GlobalSign ECC Root CA - R5
GlobalSign	GlobalSign	GlobalSign Root CA - R2	GlobalSign Extended Validation CA - SHA256 - G2 - intermediate cert being treated as root during transition
GlobalSign	GlobalSign nv-sa	Root CA	GlobalSign Root CA
GlobalSign	GlobalSign	GlobalSign Root CA - R3	GlobalSign Root CA - R3
GoDaddy	The Go Daddy Group, Inc.	Go Daddy Class 2 Certification Authority	Go Daddy Class 2 CA
GoDaddy	GoDaddy.com, Inc.		Go Daddy Root Certificate Authority - G2
GoDaddy	Starfield Technologies, Inc.	Starfield Class 2 Certification Authority	Starfield Class 2 CA
GoDaddy	Starfield Technologies, Inc.		Starfield Root Certificate Authority - G2
Google Trust Services (GTS)	GlobalSign	GlobalSign ECC Root CA - R4	GlobalSign ECC Root CA - R4

Google Trust Services (GTS)	GlobalSign	GlobalSign Root CA - R2	GlobalSign Root CA - R2
Start Commercial (StartCom) Ltd.	StartCom Ltd.	Secure Digital Certificate Signing	StartCom Certification Authority
Start Commercial (StartCom) Ltd.	StartCom Ltd.	Secure Digital Certificate Signing	StartCom Certification Authority
Start Commercial (StartCom) Ltd.	StartCom Ltd.		StartCom Certification Authority G2
Symantec	Symantec Corporation	Symantec Trust Network	Symantec Class 1 Public Primary Certification Authority - G4
Symantec	Symantec Corporation	Symantec Trust Network	Symantec Class 1 Public Primary Certification Authority - G6
Symantec	Symantec Corporation	Symantec Trust Network	Symantec Class 2 Public Primary Certification Authority - G4
Symantec	Symantec Corporation	Symantec Trust Network	Symantec Class 2 Public Primary Certification Authority - G6
Symantec / GeoTrust	GeoTrust Inc.		GeoTrust Global CA
Symantec / GeoTrust	GeoTrust Inc.		GeoTrust Global CA 2
Symantec / GeoTrust	GeoTrust Inc.		GeoTrust Primary Certification Authority
Symantec / GeoTrust	GeoTrust Inc.	(c) 2007 GeoTrust Inc. - For authorized use only	GeoTrust Primary Certification Authority - G2
Symantec / GeoTrust	GeoTrust Inc.	(c) 2008 GeoTrust Inc. - For authorized use only	GeoTrust Primary Certification Authority - G3
Symantec / GeoTrust	GeoTrust Inc.		GeoTrust Universal CA
Symantec / GeoTrust	GeoTrust Inc.		GeoTrust Universal CA 2
Symantec / VeriSign	VeriSign, Inc.	VeriSign Trust Network	VeriSign Class 1 Public PCA - G3
Symantec / VeriSign	VeriSign, Inc.	VeriSign Trust Network	VeriSign Class 2 Public PCA - G3
Symantec / VeriSign	VeriSign, Inc.	VeriSign Trust Network	VeriSign Class 3 Public Primary Certification Authority - G3
Symantec / VeriSign	VeriSign, Inc.	VeriSign Trust Network	VeriSign Class 3 Public Primary Certification Authority - G4
Symantec / VeriSign	VeriSign, Inc.	VeriSign Trust Network	VeriSign Class 3 Public Primary Certification Authority - G5

Symantec / VeriSign	VeriSign, Inc.	VeriSign Trust Network	VeriSign Universal Root Certification Authority
Trustwave	SecureTrust Corporation		Secure Global CA
Trustwave	SecureTrust Corporation		SecureTrust CA
Trustwave	XRamp Security Services Inc	http://www.xrampsecurity.com/	XRamp Global Certification Authority

11. Appendiks 1 – eksempler

Dette appendiks indeholder simple eksempler på, hvordan input og outputstrukturer kan se ud.

11.1. Inputstruktur - Besked Aflever

Eksempel på Beskedtypen "SKAT eSkattekort"

```
<?xml version="1.0" encoding="utf-8"?>
<n0:ModtagBeskedInput xmlns:n0="urn:oio:sts:1.0.0"
xmlns:prx="urn:sap.com:proxy:T85:/1SAI/TXSD9D87D84D6F3467F0332:750">
  <n1:Haendelsesbesked xmlns:n1="urn:oio:besked:kuvert:1.0">
    <n1:BeskedId>
      <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">0554b024-cd96-4fdc-a8d0-
b019abbd706a</n2:UUIDIdentifikator>
    </n1:BeskedId>
    <n1:BeskedVersion>1.0</n1:BeskedVersion>
    <n1:Beskedkuvert>
      <n1:Filtreringsdata>
        <n1:Beskedtype>
          <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">4e8be9f2-c750-48a4-af7c-
870a2b2b83f0</n2:UUIDIdentifikator>
        </n1:Beskedtype>
        <n1:BeskedAnsvarligAktoer>
          <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">d92bb9c2-d826-4028-8fb5-
d8b88b4377d4</n2:UUIDIdentifikator>
        </n1:BeskedAnsvarligAktoer>
        <n1:TilladtModtager>
          <n2:URNIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">urn:oio:cvr:35209115</n2:URNIdentifikator>
        </n1:TilladtModtager>
        <n1:ObjektRegistrering>
          <n1:ObjektRegistreringId>
            <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">20ac6dc2-9792-46d5-a508-
050f6c1a6999</n2:UUIDIdentifikator>
          </n1:ObjektRegistreringId>
          <n1:RegistreringsAktoer>
            <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">afd21f3d-11c7-4f51-b2a6-
f31d6480a9fb</n2:UUIDIdentifikator>
          </n1:RegistreringsAktoer>
          <n1:Registreringstidspunkt>
            <n2:TidsstempelDatoTid xmlns:n2="urn:oio:sagdok:3.0.0">2018-05-31T06:07:10Z</n2:Tids-
stempelDatoTid>
          </n1:Registreringstidspunkt>
          <n1:ObjektAnsvarligMyndighed>
            <n2:URNIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">urn:oio:cvr:35209115</n2:URNIdenti-
fikator>
          </n1:ObjektAnsvarligMyndighed>
          <n1:ObjektId>
            <n2:URNIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">urn:oio:dokumen-
tid:000162KSD0000000000000000000341</n2:URNIdentifikator>
          </n1:ObjektId>
          <n1:ObjektType>
            <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">3a0aaaf4-5c45-4432-9709-
f9085c86352d</n2:UUIDIdentifikator>
          </n1:ObjektType>
          <n1:ObjektHandling>
            <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">e2b30d57-504a-4e2e-ae2d-
a1394a9cb0b8</n2:UUIDIdentifikator>
          </n1:ObjektHandling>
        </n1:ObjektRegistrering>
      </n1:Filtreringsdata>
      <n1:Leveranceinformation>
        <n1:Dannelsestidspunkt>
          <n2:TidsstempelDatoTid xmlns:n2="urn:oio:sagdok:3.0.0">2018-05-31T06:07:10Z</n2:Tidsstempel-
DatoTid>
        </n1:Dannelsestidspunkt>
```

11.2. Outputstruktur - Besked Aflever

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:ModtagBeskedOutputType xmlns="urn:oio:sag-
dok:3.0.0" xmlns:ns2="urn:oio:sts:1.0.0">
  <StandardRetur>
    <StatusKode>20</StatusKode>
    <FejlbeskedTekst></FejlbeskedTekst>
  </StandardRetur>
</ns2:ModtagBeskedOutputType>
```

12. Appendiks 2 – Fejlsøgning

Dette appendiks indeholder oversigt over fejlsituationer der kan resultere i, at udvekslingen mellem Beskedfordeleren og Modtagersystemet ikke forløber planmæssigt.

Symptom	Årsag	Behandling
Der kan ikke etableres forbindelse mellem Beskedfordeleren og Modtagersystemet	Certifikatproblemer	<ul style="list-style-type: none"> - Kontroller via fanen Anvendersystem, at det endpointcertifikat Beskedfordeleren kender, er i overensstemmelse med det modtagersystemet faktisk anvender - Kontroller at trust chain er korrekt og at Beskedfordelerens certifikat er trustet. - <i>Kontroller at at 2-vejs SSL-kommunikation mellem Anvendersystemet og Beskedfordeleren er opsat korrekt.</i> - <i>Kontroller at evt load balancer har konfigureret certifikater fra Beskedfordeleren.</i>
Beskedfordeleren kalder modtagersystemets endpoint, men modtager systemet modtager ikke beskeder.	Modtagersystemet sender ikke en valid statuskode	Kontroller at der returneres valid statuskode. Slet evt. besked på køen, hvis der er fejl i den som gør, at Modtagersystemet ikke kan sende en returkode 20.
Beskedfordeleren sender den samme besked til modtagersystemet igen og igen. Beskeden bliver liggende i køen	<ol style="list-style-type: none"> 1. Skyldes at modtagersystemet ikke returnerer en korrekt "ModtagBeskedOutput" struktur. Standardretur delen er ikke tilstrækkeligt 2. Skyldes at modtagersystemet ikke returnerer en Statuskode 20/OK til Beskedfordeleren. 	Kontroller at korrekt struktur returneres med korrekt statuskode
Beskedfordeleren sender en besked der er fejlbehæftet og som modtagersystemet ikke vil modtage	Beskden bliver liggende i køen indtil statuskode 20/OK er modtaget	<ul style="list-style-type: none"> • Fejlmeld beskeden til KOMBIT • Slet de fejlbehæftede beskedtyper fra køen eller returner dem til Beskedfordelerens fejlkø eller opbevar dem i en log i eget system. Beskeder skal fjernes fra køen for ikke at stoppe den.
Tekst i UI: Rest delivery endpoint for dueslag 894beb77-0700-495b-8b4b-9ae83d159425 connection setup error: Certificate error	certifikatproblemer	<p>Kan skyldes, at et mismatch mellem det certifikat der er registreret på et endpoint i BF og det som præsenteres af serveren når endpointet kaldes</p> <p>Undesøg med en endpoint-certifikat-skanner, hvilke endpoint der faktisk udstilles. Forslag til skanner: https://www.ssllabs.com/ssltest/analyze.html</p>
I brugergrænsefladen vises en fejl i stil med nedenstående: REST delivery failure https://services-itest.xxxx/rest/api/ModtagBesked-deliveryTag: 2 Unable to parse server response : org.xml.sax.SAXParseException ;	Der sendes et tomt svar tilbage til beskedfordeleren som kvittering for at en besked er modtaget	Sørg for, at der ikke blot returneres en tom streng. Se afsnit "11.2 Outputstruktur - Besked Aflever" for eksempel på retursvar.

lineNumber: 1; columnNumber: 1; Premature end of file.		
--	--	--

13. Appendiks 3 – serviceaftale og dataafgrænsning

Sikkerhedsmodellen for støttesystemet Beskedfordeler understøtter servicesystemrollerne **Aflever** og **Modtag**. Disse roller giver Anvendersystemers adgang til at afsende til og modtage beskeder fra Beskedfordeleren.

For at have autorisation til rollerne skal Anvendersystemet tegne en serviceaftale med en myndighed i Støttesystemernes Administrationsmodul. Anvendersystemets adgang til data skal i serviceaftalen afgrænses på servicesystemrollerne via nedenstående dataafgrænsningstyper.

Dataafgrænsninger i serviceaftalen er en liste af værdier der skal matche de tilsvarende værdier i beskedkuverten for at anvendersystemet får lov til enten Aflevere eller modtage beskeder fra Beskedfordeleren. Dataafgrænsninger defineres for hver servicesystem rolle i serviceaftalen. Aflever benyttes til autorisation ved afsendelse af beskeder til beskedfordeleren. Modtag benyttes til autorisation ved distribution og modtagelse af beskeder fra Beskedfordeleren.

For hver dataafgrænsningstype kan der angives hvilke data som Anvendersystemet er autoriseret til henholdsvis at afsende eller modtage:

Dataafgrænsnings typer i Beskedfordeleren:

Dataafgrænsningstype i ADM modulet	Tilsvarende element i beskedens beskedkuvert	Tilladte værdier for dataafgrænsningstypen i serviceaftaler
Beskedtype	Filtreringsdata.Beskedtype	UUID (beskedtype kataloget) (flere værdier adskilles af komma)
Kommunalt forvaltningsområde	Objektregistrering.Opgave-Emne	Nummer i klemme klassifikationen: urn:oio:kle: [[0-9][0-9].[0-9][0-9].[0-9][0-9]] eller urn:oio:kle: [[0-9][0-9].[0-9][0-9].*] eller urn:oio:kle: [[0-9][0-9].*] urn:oio:kle:[*] (flere værdier adskilles af komma)
Følsomhed	Leveranceinformation.Sikkerhedsklassificering	UUID (se nedenstående liste)
Afsendende myndighed	Objektregistrering.ObjektAnsvarligMyndighed.	CVR nummer på 8 cifre (flere værdier adskilles af komma) urn:oio:cvr-nr:[0-9]
Ansvarlig myndighed	Filtreringsdata.TilladtModtager	Enten CVR nummer på 8 cifre (flere værdier adskilles af komma) urn:oio:cvr-nr:[0-9] eller [*]

Liste af dataafgrænsningstyper på servicesystemrollen Aflever til beskedmodtagelse og servicesystemrollen Modtag til abonnementer og beskedafgivelse i Støttesystemet Beskedfordeler.

Tilladte værdier i følsomhed:

Navn	Beskrivelse	UUID
Ikke fortrolige data	Skal forstås som: offentlige data Eksempler: navn, adresse, fødselsdato, stilling, arbejdstelefon	1d81c472-0808-44cc-963d-f5ef0170ae1d
Fortrolige personoplysninger eller fortrolige forretningsdata	Skal forstås som: ved fortrolige personoplysninger gør persondatalovens §6 sig gældende Eksempler: I. Personoplysninger: Private oplysninger om eksempelvis økonomi, hemmelig adresse, skatteforhold, gæld, sygedage, tjenestelige forhold og familieforhold II. Fortrolige forretningsdata: Agenda til et lukket møde, Energioplysninger, budgetforslag, Ud-bud(tilbudsevaluering)	292e85a9-8ad4-46df-9e50-f97d6837ad74
Følsomme personoplysninger eller følsomme forretningsdata	Skal forstås som: ved følsomme personoplysninger gør persondatalovens §7 og §8 sig gældende Eksempler: I. Følsomme personoplysninger: racemæssig / etnisk baggrund, politisk, religiøs, eller filosofisk overbevisning, fagforeningsforhold, seksuelle forhold, helbredsmæssige forhold. Strafbare forhold, væsentlige sociale problemer, andre rent private forhold. II. Følsomme forretningsdata: Forarbejde til lov, Oplysninger undtaget for aktindsigt.	31c09910-e011-46a5-86fb-254374421fe8
Særligt beskyttede oplysninger	Skal forstås som: VIP-sager og kritiske forretningsdata Eksempler: I. VIP sager: De kongelige, politikere etc. II. Kritiske forretningsdata: Forsvarets bygninger	44f4108b-26d4-46de-a90f-35e35b55b8d8

Liste af mulige værdier i dataafgrænsningstypen følsomhed (sikkerhedsklassificering i beskedkuverten)

Serviceaftale autorisation data's sammenhæng med data i beskedkuverten :



Figuren viser sammenhængen mellem data i serviceaftaler og beskeder for henholdsvis aflevering og modtagelse af beskeder

Serviceaftaler med Beskedfordelerens servicesystemroller provisioneres fra Administrationsmodulet til både støttesystemernes system til adgangsstyring for systemer (STS) og til Beskedfordeleren. STS omdanner serviceaftalerne til sikkerhedstokens der anvendes som "bevis" af anvendersystemets autorisation ved kald af Beskedfordelerens besked services.

Dataafgrænsnings type i serviceaftale i sikkerhedstoken	Attribut i beskedkuverten	Autorisations regler for Aflever rollen når en besked modtages i Beskedfordeleren
Privelegegroup scope (Anvender kontekst fra serviceaftalen)	ObjektAnsvarligMyndighed	-ObjektAnsvarligMyndighed I beskeden skal være identisk med et privelegegroup scope i token -Hvis ObjektAnsvarligMyndighed ikke er udfyldt i beskedkuverten bliver der ikke afgrænset for privelegegroup scope i token
Beskedtype	Beskedtype	Beskedtypen i beskedkuverten skal eksistere i listen af tilladte beskedtyper i tokenet
Kommunalt_forvaltningsomraade	OpgaveEmne	-OpgaveEmne i beskeden skal eksistere i listen af tilladte kommunale_forvaltningsomraader i tokenet -Hvis Opgaveemne I beskedkuverten ikke er udfyldt bliver der ikke afgrænset for Kommunalt_forvaltningsomraade -Hvis der ikke afgrænses for Kommunalt_forvaltningsomraade i tokenet må Opgaveemne ikke være udfyldt i beskedkuverten. -Hvis der i tokenet afgrænses for Kommunalt_forvaltningsomraade med '*' må Opgaveemne have alle gyldige værdier i beskedkuverten.
Følsomhed	Sikkerhedsklassificering	-Sikkerhedsklassificering i beskedkuverten skal være lig med eller mindre end Følsomhed i tokenet -Hvis Sikkerhedsklassificering i beskedkuverten ikke er udfyldt bliver der ikke afgrænset for Følsomhed

		-Hvis der ikke afgrænses for Foelsomhed i tokenet må Sikkerhedsklassificering ikke være udfyldt i beskedkuverten.
Ansvarlig_myndighed	TilladtModtager	-Alle værdier i TilladtModtager i beskedkuverten skal findes i listen af Ansvarlig_myndighed i tokenet -Hvis TilladtModtager i beskedkuverten ikke er udfyldt bliver der ikke afgrænset for Ansvarlig_myndighed. -Hvis der ikke afgrænses for Ansvarlig_myndighed i tokenet må TilladtModtager ikke være udfyldt i beskedkuverten.

Tabel over Dataafgrænsningstyper i serviceaftaler og de matchende attributter i beskedkuverten. Autorisations-regler for hver dataafgrænsningstype for Aflever-rollen når en besked modtages i Beskedfordeleren. Betydning og placering af de enkelte attributter i beskedkuverten fremgår af dokumentet B.08.09 Underbilag 20 Beskedkuvert. Hvis attributtens tags er angivet i beskedkuverten men uden indhold opfattes attributten som udfyldt.

Dataafgrænsningstype i den provisionerede serviceaftale	Attribut i beskedkuverten	Autorisations-regler for Modtag-rollen når en besked distribueres til modtagersystemers dueslag i Beskedfordeleren
Anvenderkontekst i provisionerede data (myndighed i serviceaftalen)	TilladtModtager	-Minst en TilladtModtager i beskedkuverten skal være blandt scope i anvendersystemets serviceaftaler -Hvis TilladtModtager ikke er udfyldt i beskedkuverten bliver der ikke afgrænset for scope i anvendersystemets serviceaftaler. Det betyder, at alle anvendersystemer kan tegne abonnement på beskeden.
Beskedtype	Beskedtype	Beskedtypen i beskedkuverten skal eksistere i listen af tilladte beskedtyper i anvendersystemets serviceaftale
Kommunalt_forvaltningsomraade	OpgaveEmne	-OpgaveEmne i beskedkuverten skal eksistere i listen af tilladte kommunalt_forvaltningsomraader i tokenet -Hvis Opgaveemne i beskedkuverten ikke er udfyldt bliver der ikke afgrænset for Kommunalt_forvaltningsomraade -Hvis der ikke afgrænses for Kommunalt_forvaltningsomraade i serviceaftalen må Opgaveemne ikke være udfyldt i beskedkuverten. -Hvis der i serviceaftalen afgrænses for Kommunalt_forvaltningsomraade med '*' må Opgaveemne have alle gyldige værdier i beskedkuverten.
Foelsomhed	Sikkerhedsklassificering	-Sikkerhedsklassificering i beskedkuverten skal være lig med eller mindre end Foelsomhed i serviceaftalen -Hvis Sikkerhedsklassificering i beskedkuverten ikke er udfyldt bliver der ikke afgrænset for Foelsomhed

		-Hvis der ikke afgrænses for Foelsomhed i serviceaftalen må Sikkerhedsklassificering ikke være udfyldt i beskedkuverten.
Afsendende_myndighed	ObjektAnsvarligMyndighed	-ObjektAnsvarligMyndighed I beskedkuverten skal være identisk med en Afsendende_myndighed i serviceaftalen -Hvis ObjektAnsvarligMyndighed ikke er udfyldt i beskedkuverten bliver der ikke afgrænset for Afsendende_mundighed -Hvis der ikke afgrænses for Afsendende_myndighed i serviceaftalen må ObjektAnsvarligMyndighed ikke være udfyldt i beskedkuverten.

Tabel over Dataafgrænsningstyper i serviceaftaler der er provisioneret fra administrationsmodulet til Beskedfordelern og de matchende attributter i beskedkuverten. Autorisations-regler for hver dataafgrænsningstype for Modtag-rollen når en besked distribueres i Beskedfordelern. Betydning og placering af de enkelte attributter i beskedkuverten fremgår af dokumentet B.08.09 Underbilag 20 Beskedkuvert. Hvis attributtens tags er angivet i beskedkuverten men uden indhold opfattes attributten som udfyldt.