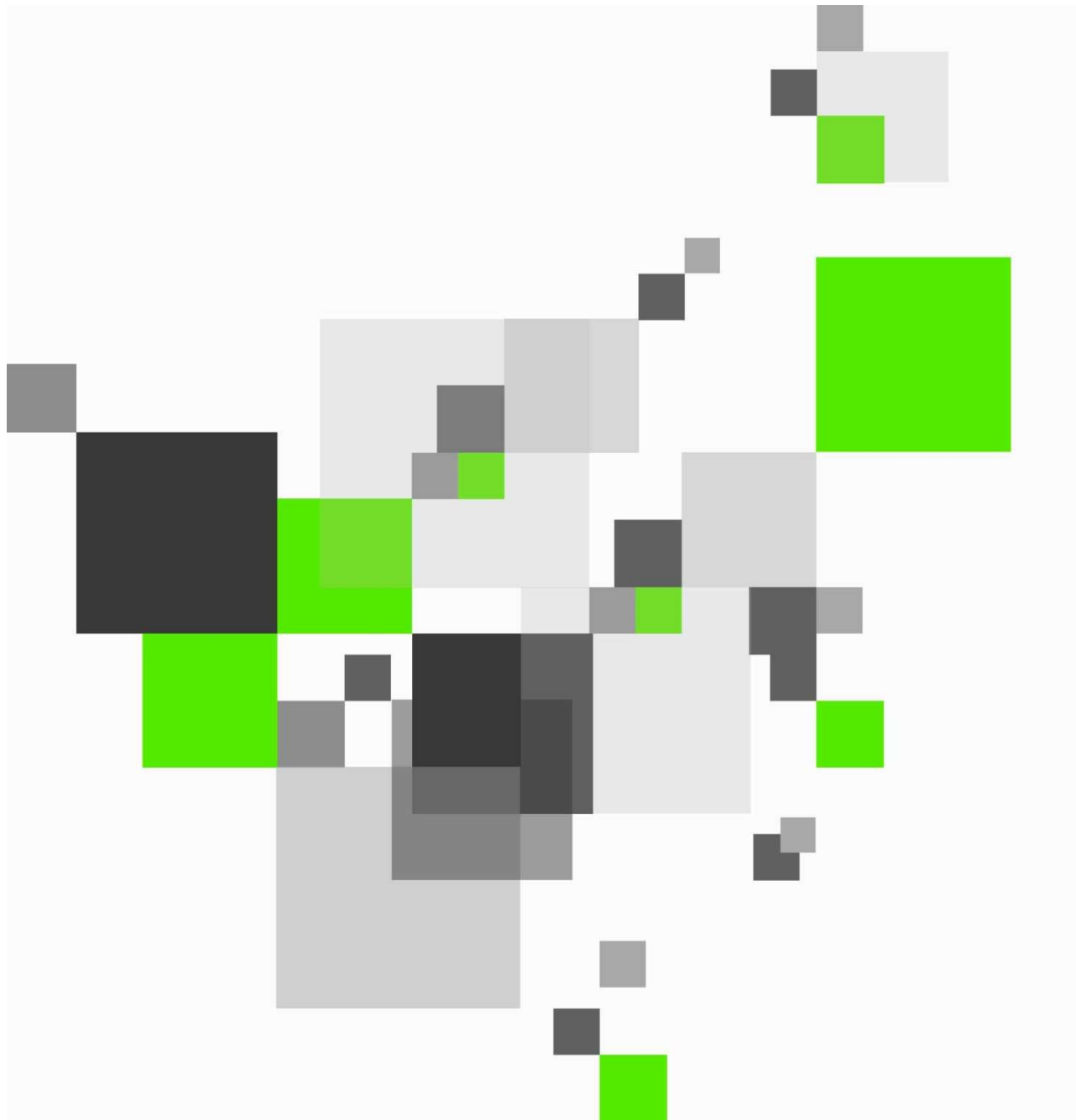


## Besked-FåTilsendt-Snitflade



## Indholdsfortegnelse

<b>Historik .....</b>	<b>3</b>
<b>1. Versioner .....</b>	<b>5</b>
<b>2. Målgruppe .....</b>	<b>5</b>
<b>3. Snitfladebeskrivelse for SF1461 – BeskedFåTilsendt .....</b>	<b>5</b>
<b>4. Servicebeskrivelse .....</b>	<b>5</b>
<b>5. Funktionalitet i servicen BeskedFåTilsendt .....</b>	<b>6</b>
5.1. Inputdokument .....	6
5.2. Outputdokument .....	7
<b>6. Teknisk beskrivelse .....</b>	<b>8</b>
6.1. Sikkerhed .....	8
6.2. SecurityPolicy .....	8
6.3. Certifikater .....	8
6.4. Autorisation .....	9
6.5. Skemavalidering .....	9
<b>7. Kommunikation .....</b>	<b>9</b>
7.1. Håndtering af utilgængelighed i snitfladen .....	9
7.2. Angivelse af transaktionsId i snitfladen .....	10
<b>8. Eventuelt yderligere oplysninger .....</b>	<b>10</b>
<b>9. Appendiks 1 - trusted certifikatudstedere for endpoint SSL .....</b>	<b>11</b>
<b>10. Appendiks 2 – eksempler .....</b>	<b>15</b>
10.1. Inputstruktur - Besked FåTilsendt .....	15
10.2. Outputstruktur – Besked FåTilsendt .....	17
<b>11. Appendiks 3 – Fejlsøgning .....</b>	<b>18</b>

## 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 " <b>Modtag besked</b> " til " <b>Modtagbesked</b> "	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

2022-05-18	7.0	AXB	LetsEncrypt certifikater tilføjet til liste over godkendte certifikater. Jf. SRITM0885306	2.8
2022-07-28	7.2	AXB	Kapitel 3, 6, 9 er opdateret i forbindelse med VA-150.	2.8
2022-08-02	7.3	AXB	Sektion om certifikater opdateret med specificering af forskel på test og produktions certifikater.	2.8
2022-08-19	7.5	AXB	Service omdøbt fra AfleverBesked til BeskedFåTilsendt	2.8
2022-10-03	8.0	AXB	Konsekvensrettet og reviewet i forbindelse med generel opdatering af Beskedfordeler dokumentation. Ingen ændringer i funktionalitet.	2.8

## 1. Versioner

Snitfladens version er 1.0.0

- Service specifikation: Anvendersystem.wadl

## 2. Målgruppe

Integrationsudviklere der arbejder hjemmenvant med SOAP og REST teknologier.

## 3. Snitladebeskrivelse for SF1461 – BeskedFåTilsendt

Nærværende dokument beskriver, hvorledes en service, **BeskedFåTilsendt**, 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 **Fælleskommunalt Administrationsmodul**, som et callback endpoint konfigureret for **Modtagersystemet**.



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

Information omkring specifikke endpoints kan til enhver tid findes på Digitaliseringskataloget under SF1461.

## 4. Servicebeskrivelse

For at **Beskedfordeler** kan aflevere beskeder til **Anvendersystemerne**, skal de implementere denne REST web service. I **Anvendersystemernes** snitladebeskrivelser, 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 servicen BeskedFåTilsendt

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 **HændelsesBesked** 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 2 – eksempler" afsnit "10.1 Inputstruktur - Besked FåTilsendt" 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 (<b>Beskedkuvert.xsd</b>), 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 2 – eksempler" afsnit "10.2 Outputstruktur – Besked FåTilsendt" er der eksempler på, hvordan outputstrukturen kan se ud. I "Appendiks 3 – 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 **Modtagersystemet** 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 være udstedt af en af leverandørerne fra "Appendiks 1 - trusted certifikatudstedere for endpoint SSL". Der skal benyttes SSL certifikater til at beskytte endpointet.
- at der anvendes TLS version 1.2.

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

. Denne service er af type "**Simple callback service**", hvor Servicen autentificerer anvendersystemet 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 skal beskyttes med 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 det provisionerede certifikat til endpointet for at sikre at endpointet faktisk er ejet af det system som også ejer dueslaget.

For at kunne modtage beskeder fra **Beskedfordeler** er det vigtigt at modtagersystemet truster **Beskedfordelers** funktionscertifikat. Hvilket certifikat der her er tale om afhænger af det miljø som modtagersystemet befinder sig i. Der findes separate certifikater til miljøerne Ekstern Test og Produktion. De nyeste certifikater til begge miljøer kan til enhver tid findes på [Digitaliseringskataloget](#).



## 6.4. Autorisation

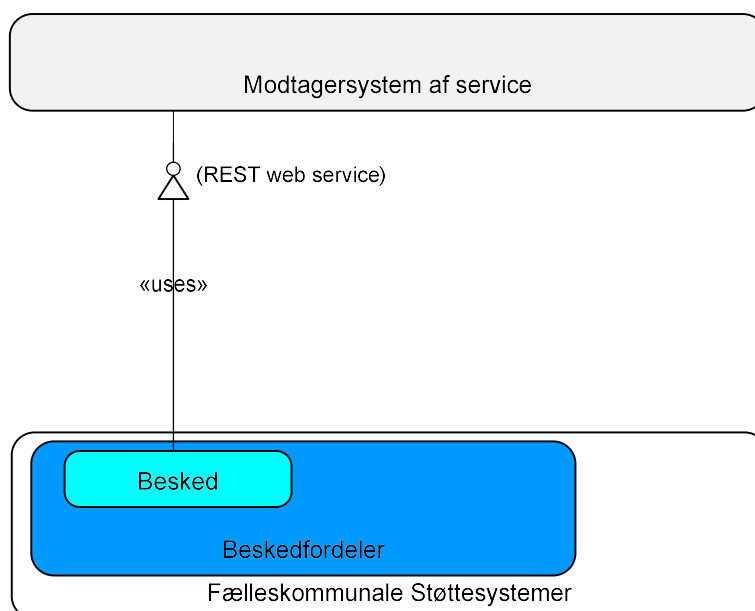
**Beskedfordeler** autoriseres til at kalde snitfladen ved, at **Beskedfordeler**s certifikat er velkendt af **Modtagersystemet**. Mulighederne for dataafgrænsninger gældende for abonnementer der kan filtrere de beskeder der kan hentes via snitfladen er beskrevet i SF1461 – Modtag beskeder via Beskedfordeler

## 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-FåTilsendt-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 f.eks. 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. Eventuelt yderligere oplysninger

Yderligere information og dokumentation om snitfladen kan findes i [Digitaliseringskataloget under SF1461](#). Dette inkluderer også en liste over alle endpoints relateret til snitfladen.

## 9. Appendiks 1 - trustede certifikatstedere 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	<a href="http://www.usertrust.com/">http://www.usertrust.com/</a>	UTN-USERFirst-Client Authentication and Email
Comodo	The USERTRUST Network	<a href="http://www.usertrust.com/">http://www.usertrust.com/</a>	UTN-USERFirst-Hardware
Comodo	The USERTRUST Network	<a href="http://www.usertrust.com/">http://www.usertrust.com/</a>	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	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert Assured ID Root CA
DigiCert	DigiCert Inc	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert Assured ID Root G2
DigiCert	DigiCert Inc	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert Assured ID Root G3

DigiCert	DigiCert Inc	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert Global Root CA
DigiCert	DigiCert Inc	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert Global Root G2
DigiCert	DigiCert Inc	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert Global Root G3
DigiCert	DigiCert Inc	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert High Assurance EV Root CA
DigiCert	DigiCert Inc	<a href="http://www.digicert.com/">http://www.digicert.com/</a>	DigiCert Trusted Root G4
Entrust	AffirmTrust		AffirmTrust Commercial
Entrust	AffirmTrust		AffirmTrust Networking
Entrust	AffirmTrust		AffirmTrust Premium
Entrust	AffirmTrust		AffirmTrust Premium ECC
Entrust	Entrust, Inc.	<a href="http://www.entrust.net/CPS%20is%20incorporated%20by%20reference">www.entrust.net/CPS is incorporated by reference</a>	Entrust Root Certification Authority
Entrust	Entrust, Inc.	<a href="http://www.entrust.net/legal-terms">See www.entrust.net/legal-terms</a>	Entrust Root Certification Authority - EC1
Entrust	Entrust, Inc.	<a href="http://www.entrust.net/legal-terms">See www.entrust.net/legal-terms</a>	Entrust Root Certification Authority - G2
Entrust	<a href="http://Entrust.net">Entrust.net</a>	<a href="http://www.entrust.net/CPS%202048%20in%20corp.%20by%20ref.%20limits%20liab.%20">www.entrust.net/CPS 2048 in-corp. by ref. (limits liab.)</a>	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	<a href="http://GoDaddy.com, Inc.">GoDaddy.com, Inc.</a>		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
Internet Security Research Group	Letsencrypt.org	<a href="https://letsencrypt.org/certificates/">https://letsencrypt.org/certificates/</a>	ISRG Root X1
Internet Security Research Group	Letsencrypt.org	<a href="https://letsencrypt.org/certificates/">https://letsencrypt.org/certificates/</a>	Let's Encrypt R3
Internet Security Research Group	Letsencrypt.org	<a href="https://letsencrypt.org/certificates/">https://letsencrypt.org/certificates/</a>	ISRG Root X2
Internet Security Research Group	Letsencrypt.org	<a href="https://letsencrypt.org/certificates/">https://letsencrypt.org/certificates/</a>	Let's Encrypt E1
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	<a href="http://www.xrampsecurity.com/">http://www.xrampsecurity.com/</a>	XRamp Global Certification Authority

## 10. Appendiks 2 – eksempler

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

### 10.1. Inputstruktur - Besked FåTilsendt

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>
  <n1:TransaktionsId>
    <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">7f969aff-1b75-4829-be53-
3b4c8d7b9366</n2:UUIDIdentifikator>
  </n1:TransaktionsId>
  <n1:Kildesystem>
    <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">d6d76e7e-326e-4c23-8ef4-
84752dc588a9</n2:UUIDIdentifikator>
  </n1:Kildesystem>
  <n1:KildesystemIPAdresse>::FFFF:172.30.217.227</n1:KildesystemIPAdresse>
  <n1:KildesystemAkkreditiver>U0VSSUFMTIVNqkVSPUNWUjoxOTQzNTA3NS1GSUQ6Mjg3NjQwNTYgKyB-
DTj1Lb21iaXQtU1BGLXRlc3Qtc3RzLVNpa2tIcmhlZCAoZnVua3Rpb25zY2Vy dGlmaWthdCksIE89S09NQklUIEEvUyAvLyB-
DVII6MTk0MzUwNzUsIEM9REs=.MTQ0OTAwOTE4Mw==.Q049VFJU1QyNDAA4IFN5c3RlbXRlc3QgWEIYIEN-
BLCBPPVRSVNUMjQwOCwgQz1ESw==</n1:KildesystemAkkreditiver>
  <n1:Sikkerhedsklassificering>
    <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">1d81c472-0808-44cc-963d-
f5ef0170ae1d</n2:UUIDIdentifikator>
  </n1:Sikkerhedsklassificering>
  <n1:Leveranceruter>
  <n1:Leverancerute>
    <n1:Fordelingssystem>
      <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">f9fbbb38-4b2f-11e5-885d-
feff819cdc9f</n2:UUIDIdentifikator>
    </n1:Fordelingssystem>
    <n1:ModtagelsesTidspunkt>
      <n2:TidsstempelDatoTid xmlns:n2="urn:oio:sagdok:3.0.0">2018-05-
31T06:10:08Z</n2:TidsstempelDatoTid>
    </n1:ModtagelsesTidspunkt>
    <n1:LeveranceTidspunkt>
      <n2:TidsstempelDatoTid xmlns:n2="urn:oio:sagdok:3.0.0">2018-05-
31T06:10:08Z</n2:TidsstempelDatoTid>
    </n1:LeveranceTidspunkt>
    <n1:ModtagetFraSystem>
      <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">d6d76e7e-326e-4c23-8ef4-
84752dc588a9</n2:UUIDIdentifikator>
    </n1:ModtagetFraSystem>
    <n1:ErLeveretIHenholdTil>
      <n2:UUIDIdentifikator xmlns:n2="urn:oio:sagdok:3.0.0">e9f8b88f-e1c5-432f-b309-
987a739a3556</n2:UUIDIdentifikator>
    </n1:ErLeveretIHenholdTil>
    <n1:LeveranceruteLokalUdvidelse>
      <n1:AntalLeveranceforsoeg>1</n1:AntalLeveranceforsoeg>
    </n1:LeveranceruteLokalUdvidelse>
  </n1:Leverancerute>
</n1:Leveranceruter>
</n1:Leveranceinformation>
<n1:GyldighedFra>
  <n2:TidsstempelDatoTid xmlns:n2="urn:oio:sagdok:3.0.0">2018-05-30T11:39:44Z</n2:Tidsstempel-
DatoTid>
  </n1:GyldighedFra>
</n1:Beskedkuvert>
<n1:Beskeddata>
  <Base64 content-type="text/plain" encoding="ISO-8859-1" file-type=".xml" xmlns:ns5="urn:oio:sag-
dok:3.0.0" xmlns:ns4="urn:oio:sagdok:3.0.0">PFN0YXR1c1ByaW50QmVza2VkIHhtbG5zPSJodHRwOi8vc2Vy d-
mljZXBsYXRmb3JtZW4uZGsveG1sL3ByaW50L1ByaW50U3Rh dHVzLzEvdEdHlwZXMiPjxBZnNlbnRlbnHNISWRlbnRpZm l-
rYXRvcj4wMDAxNjlLU0QwMDAwMDAwMDAwMDAwMDAzNDE8L0Fmc2VuZGVsc2VJZGVudGlmaWthdG9yPjxGb3Jz
ZW5kZWxzZUl kZW50aWZpa2F0b3I+MTAxNTg3NzwvRm9yc2VuZGVsc2VJZGVudGlmaWthdG9yPjxLYW5hbEtvZGU+Rnl-
zaXNrIFBvc3Q8L0thbmFsS29kZT48QWZzZW5kZWxzZU1vZHRhZ2VyPjEx-
MDQ1NjQ2ODk8L0Fmc2VuZGVsc2VNbnR0YWdlcj48QWZzZW5kZWxzZU1vZHRhZ2VyVHlwZT5DchI8L0Fmc2VuZGVsc2V
Nb2R0YWdlclR5cGU+PFBlcnNvb3k5ShbWU+U3VzYW5uZSBBNYw5nZWxrasOmcjwvUG-
Vyc29uTmFtZT48VHJhbnNha3Rpb25zRGF0b1RpZD4yMDE4LT A1LT MvVDE-
zoJM5OjQ0LjA0MzU2Njk8L1RyYU5zYWt0aW9uc0Rh dG9UaWQ+PEFmc2VuZGVyU3lzdGVtSWRlbnRpZm l-
rYXRvcj4xNj18L0Fmc2VuZGVyU3lzdGVtSWRlbnRpZm lrYXRvcj48VHJhbnNha3Rpb25zU3Rh dHVzS29kZT5LbGFyPC9Ucm F
uc2Fr dGlbnNTdGF0dXNl b2RI PjxGb3JzZW5kZWxzZVR5cGVJZGVudGlmaWthdG9yPjY5NTwwRm9yc2VuZGVsc2VUeX-
BISWRlbnRpZm lrYXRvcj48Q29ycmVsYXRpb25JZD4yMGFjNmRjMi05Nzk yLTQ2ZDUtYTUwOC0wNT-
BmNmMxYTY5OTk8L0NvcnJlbGF0aW9uSUwQ+PC9TdGF0dXNQcm ludeJl c2tiZD4=</Base64>
</n1:Beskeddata>
```



---

```
</n1:Haendelsesbesked>  
</n0:ModtagBeskedInput>
```

## 10.2. Outputstruktur – Besked FåTilsendt

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<ns2:ModtagBeskedOutput 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>
```

## 11. Appendiks 3 – 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"> <li>- Kontroller via fanen Anvendersystem, at det endpointcertifikat Beskedfordeleren kender, er i overensstemmelse med det modtagersystemet faktisk anvender</li> <li>- Kontroller at trust chain er korrekt og at Beskedfordelerens certifikat er trustet.</li> <li>- <i>Kontroller at at 2-vejs SSL-kommunikation mellem Anvendersystemet og Beskedfordeleren er opsat korrekt.</i></li> <li>- <i>Kontroller at evt load balancer har konfigureret certifikater fra Beskedfordeleren.</i></li> </ul>
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"> <li>1. Skyldes at modtagersystemet ikke returnerer en korrekt "ModtagBeskedOutput" struktur. Standardretur delen er ikke tilstrækkeligt</li> <li>2. Skyldes at modtagersystemet ikke returnerer en Statuskode 20/OK til Beskedfordeleren.</li> </ol>	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"> <li>• Fejlmeld beskeden til KOMBIT</li> <li>• 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.</li> </ul>
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: <a href="https://www.ssllabs.com/ssltest/analyze.html">https://www.ssllabs.com/ssltest/analyze.html</a></p>
I brugergrænsefladen vises en fejl i stil med nedenstående: REST delivery failure <a href="https://services-itest.xxxxx/rest/api/Modtag-Besked">https://services-itest.xxxxx/rest/api/Modtag-Besked</a> deliveryTag: 2 Unable to parse server response : org.xml.sax.SAXParseException; lineNumber: 1; columnNumber: 1; Premature end of file.	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 "10.2 Outputstruktur – Besked FåTilsendt" for eksempel på retursvar.