Digitaliserings-
styrelsen

Bilag 3a) Tilslutningsvejledning for danske myndigheder til OOTS-gatewayen (DKD)

Tekniske forudsætninger og krav ved direkte integration til OOTS-gateway

Sidst opdateret 19.03.2026

Version 1.0

Introduktion

Denne vejledning henvender sig til it-ansvarlige og tekniske medarbejdere i danske myndigheder, som ønsker at tilslutte sig OOTS-gatewayen via direkte integration. Vejledningen skal læses i forlængelse af bilag 3: Introduktion til OOTS-integration, som overordnet beskriver den forretningsmæssige kontekst og forudgående tilslutningsproces.

Før du begynder

Denne vejledning henvender sig til myndigheder der ønsker en direkte integration via Digitaliseringsstyrelsen. Se venligst hoveddokumentet "Introduktion til OOTS-implementering" for at sikre at den direkte integration er den rette implementeringsvej for myndigheden, som denne tilslutningsvejledning beskriver.

Denne vejledning tager ikke højde for EU-kommissionens krav til indholdet af beskeder, men hvordan beskeder kan sendes mellem myndighedens system og Digitaliseringsstyrelsens OOTS-gateway. Myndighedernes system skal kunne formatere indholdet af beskeder i overensstemmelse med disse krav. Vejledning herom kan findes i bilag 5: Guide til OOTS-hub og EU tekniske specifikationer.

For at sikre, at myndighedens selvbetjeningsløsning kan indhente den korrekte information, skal den først registreres i EU's centrale katalogtjeneste, *Common Services.* Her kobles selvbetjeningsløsningen til de relevante EU OOTS-procedurer og -dokumentationskrav.

Digitaliseringsstyrelsen er ansvarlig for at administrere de danske data i *Common Services.* For at få registreret myndighedens selvbetjeningsløsning i Common Services skal myndigheden kontakte Digitaliseringsstyrelsen for en tilslutningsaftale, se også bilag 3 Introduktion til OOTS-integration afsnit 3. Myndigheder, der implementerer selvbetjeningsløsninger som anmodere om dokumentation, skal også implementere opslag i Common Services til identifikation af relevante dokumentationstyper og udstedere. Vejledning herom kan findes i bilag 5: Guide til OOTS-hub og EU tekniske specifikationer, del 1. afsnit 3. og 4.

Tekniske forudsætninger og krav ved direkte integration til OOTS-gateway

Myndigheder, der ønsker at etablere en direkte integration til OOTS-gatewayen, skal opfylde en række tekniske forudsætninger. Disse krav sikrer, at kommunikationen lever op til kravene om sikkerhed, interoperabilitet og korrekt routing i det europæiske OOTS-netværk.

Kommunikation over HTTPS (Direct Trust)

Kommunikationen mellem myndighedens system og Digitaliseringsstyrelsens OOTS-gateway foregår via HTTPS med Direct Trust-model. Det indebærer:

- Brug af gensidigt godkendte certifikater (Fx udstedt af Statens IT).
- Whitelisting af certifikatet efter udveksling med Digitaliseringsstyrelsen.
- Etablering af TLS-forbindelse, hvor både klient og server validerer hinandens certifikater (mutual TLS).

Myndigheden skal sikre, at certifikatet:

- Overholder gældende standarder for kryptering og nøglelængde.
- Er gyldigt i hele integrationsperioden og kan fornyes rettidigt.
- Matcher det domæne og endpoint, der anvendes.

Certifikaterne anvendes til:

- Transport-sikkerhed (TLS).
- Meddelelsessignering i AS4 (XML-digital signature).
- Kryptering af meddelelser i AS4.

Endpoints for direkte integration

Digitaliseringsstyrelsen stiller følgende AS4-endpoints til rådighed for danske myndigheder, der ønsker direkte integration til OOTS:

Miljø	Endpoint URL	Formål
Acceptance	https://oots-dk-ap-acc.digst.govcloud.dk/domibus/services/msh	Test
Produktion	https://oots-dk-ap.digst.govcloud.dk/domibus/services/msh	Drift

Alle anmodninger skal sendes til ovenstående eDelivery endpoints afhængigt af miljø.

Bemærk: Det er Digitaliseringsstyrelsens OOTS-gateway, der varetager videresendelse af beskeder til relevante EU-access points. Myndigheder, der tilslutter sig, skal ikke selv etablere forbindelse til det europæiske netværk, men alene sikre korrekt afsendelse til den danske OOTS gateway.

Routing og videresendelse håndteres automatisk af gatewayen baseret på OOTS-standarder og metadata i meddelelsen (f.eks. trackingIdentifier).

OOTS-registrerings ID og brug i OriginalSender

Ved tilslutning oplyses til Digitaliseringsstyrelsen et unikt *OOTS-registrerings ID*, som myndigheden skal anvende i AS4-headeren OriginalSender. Dette ID bruges til at identificere den afsendende myndighed entydigt i både dansk og europæisk kontekst. Det unikke *OOTS-registrerings ID* er fastlagt af myndigheden og dokumenteret i myndighedens tilslutningsaftale med Digitaliseringsstyrelsen, læs mere herom i Introduktion til OOTS-introduktion (bilag 3).

- Format: Fastlagt af EU (https://docs.peppol.eu/edelivery/codelists/ dog uden 99XX værdier).
- Skal anvendes konsekvent i alle anmodninger.
- Skal registreres i gatewayens konfiguration (tilslutningsmodul).
- Skal være unikt og fastlagt af myndigheden som en af følgende EAS-typer:
    - 0184 - CVR nummer (myndighedens primære løsning)
    - 0096 - P-nummer (myndighedens sekundære løsning som er tilknyttet et p-nummer)
    - 0088 - GLN nummer (myndighedens yderligere løsninger)
- Skal være kommunikeret til Digitaliseringsstyrelsen via myndighedens tilslutningsaftale.

P-mode-konfiguration

P-mode er en central del af AS4-konfigurationen og definerer, hvordan meddelelser skal sendes, modtages og behandles. Hver myndighed skal:

- Udarbejde eller tilpasse P-mode-filer til deres Domibus-instans
- Sikre at værdier som Service, Action, PartyId, OriginalSender, FinalRecipient er korrekt konfigureret
- Koordinere værdier med Digitaliseringsstyrelsen for at sikre korrekt routing

Et eksempel på en P-mode-fil er vedlagt som bilag 3a,i) til denne vejledning.

AS4-headere og meddelelsesstruktur

For at sikre korrekt behandling og routing af meddelelser gennem OOTS-gatewayen skal en række AS4-headere udfyldes korrekt. Disse felter udgør en

del af SOAP/ebMS3-headeren og skal være i overensstemmelse med OOTS-specifikationerne og den konfigurerede P-mode.

Centrale AS4-headere

Felt	Beskrivelse
MessageId	Unik identifikator for hver meddelelse
PartyInfo.From.PartyId	Identifikator for Access Point som myndigheden anvender
PartyInfo.To.PartyId	Acceptance: oots_dk_ap_acc Produktion: oots_dk_ap_prod
PartyInfo.From.Role PartyInfo.To.Role	http://sdg.europa.eu/edelivery/gateway
CollaborationInfo.Service	Fastsat tjeneste, fx EvidenceService
CollaborationInfo.Action	Handlingstype, fx SubmitEvidenceRequest
originalSender	Det oplyste *OOTS-registrerings ID* af myndigheden
finalRecipient	Identifikator for modtagende myndighed i EU
trackingIdentifier	Indeholder PartyInfo.To.PartyId og bruges til at bestemme, hvilket EU-access point beskeden skal sendes til. Værdien hentes fra Common Services

Alle værdier, der vedrører parter, roller, tjenester og handlinger, skal være defineret i den P-mode XML, der uploades til Domibus. Se bilag 2a,i).

Brug af trackingIdentifier til overførsel af PartyInfo.to.PartyID (midlertidig løsning)

I den nuværende danske løsning anvendes feltet trackingIdentifier til overførsel af PartyInfo.To.PartyId og bruges til at bestemme, hvilket EU-access point beskeden skal sendes til. Værdien hentes fra Common Services. Dette er en midlertidig løsning og ikke nødvendigvis en blivende del af specifikationen for den danske del af OOTS-netværket.

Det er vigtigt, at myndigheder er opmærksom på, at:

- TrackingIdentifier anvendes udelukkende som en intern løsning i den danske OOTS-gateway.
- Feltet kan ændres eller helt udgå i kommende versioner af løsningen. Det kan fx blive aktuelt, såfremt eDelivery tilslutning til OOTS-Gateway tilpasses NemHandel infrastrukturen.

Vigtige tekniske krav

- PartyIdType skal sættes til: urn:cef.eu:names:identifier:EAS:[code] (hvis myndigheden har EAS-kode), ellers urn:oasis:names:tc:ebcore:partyid-type:unregistered:DA
- Rollen (Role) er altid: http://sdg.europa.eu/edelivery/gateway
- MEP (Message Exchange Pattern) skal være: http://www.oasis-open.org/committees/ebxml-msg/one-way
- Brug følgende leg-konfigurationer i P-mode:
    - ootsRequestLeg
    - ootsResponseLeg
    - ootsErrorLeg (valgfrit)
- Certifikatets Common Name (CN) skal matche PartyName i P-mode
- Firewall skal tillade HTTPS-trafik på port 443 til:
    - Acceptance: https://oots-dk-ap-acc.digst.govcloud.dk/domibus/services/msh
    - Produktion: https://oots-dk-ap.digst.govcloud.dk/domibus/services/msh

Ved etablering af forbindelse bør der koordineres et teknisk opstartsmøde med Digitaliseringsstyrelsen for:

- Afstemning af P-mode og certifikatkonfiguration.
- Test af AS4-kommunikation.
- Gennemgang af headers og fejlscenarier.
- End-to-end test med fx Finland (hvis relevant for myndigheden).

Praktiske krav til etablering af forbindelse

For at sikre en stabil og valid kommunikationsforbindelse til OOTS-gatewayen er der en række tekniske og konfigurationsmæssige krav, som bør være opfyldt før test og drift:

P-mode konfiguration

- PartyId, PartyName og Endpoint skal matche 100% på begge sider (myndighed og Digitaliseringsstyrelsen).
- PartyIdType skal være: urn:cef.eu:names:identifier:EAS:[code] hvis EAS-kode findes, ellers urn:oasis:names:tc:ebcore:partyid-type:unregistered:DA.
- Rollerne i From/To sættes til: http://sdg.europa.eu/edelivery/gateway (både initiator og responder).
- Brug følgende leg-konfigurationer:
    - ootsRequestLeg
    - ootsResponseLeg
    - ootsErrorLeg (valgfri til fejlhåndtering)

Property-konfiguration

Følgende properties skal defineres i P-mode og sendes med meddelelser:

<property name="originalSenderProperty" key="originalSender"
datatype="string" required="true"/>
<property name="finalRecipientProperty" key="finalRecipient" datatype="string"
required="true"/>
<property name="trackingIdentifier" key="trackingIdentifier" datatype="string"
required="true"/>
Disse grupperes i et PropertySet, fx:
<propertySet name="fourCornersPropertySet">
<propertyRef property="originalSenderProperty"/>
<propertyRef property="finalRecipientProperty"/>
<propertyRef property="trackingIdentifier"/>
</propertySet>

Certifikater og trust

- Certifikatets CN/navn skal matche PartyName i P-mode.
- Certifikater skal være korrekt installeret i både keystore og truststore.
- Keystore skal indeholde myndighedens private nøgle.
- Truststore skal indeholde Digitaliseringsstyrelsens certifikat (og omvendt).

Adgang og netværk

- Endpoint skal være tilgængeligt over HTTPS.
- Følgende skal være sikret:
  - IP-adgang og firewall-regler på begge sider.
  - Port 443 skal være åben for indgående og udgående trafik.
  - DNS-navn skal være oplyst korrekt.
- I testmiljøet (acceptance) anvendes: https://oots-dk-ap-acc.digst.govcloud.dk/domibus/services/msh

Fejlhåndtering og validering

- Brug trackingIdentifier som midlertidigt ID til routing og intern debug.
- Vær opmærksom på, at nogle fejl, f.eks. med preview-parametre, kræver korrekt requestId i re-send scenarier.
- Digitaliseringsstyrelsen kan i testfasen manuelt mappe værdier, men automatisering implementeres frem mod produktion.

Overblik over OOTS-netværket og arkitekturen

OOTS-infrastrukturen er udviklet til at understøtte sikker og pålidelig dataudveksling mellem offentlige myndigheder i EU. For danske myndigheder sker adgangen til det europæiske netværk via Digitaliseringsstyrelsens OOTS-gateway, som fungerer som nationalt adgangsknudepunkt. Dette afsnit giver et samlet overblik over den tekniske arkitektur og kommunikationsflow.

Arkitektonisk opbygning

OOTS-netværket består af:

- Nationale gateways med eDelivery access points (typisk baseret på Domibus med AS4-protokol).
- EU's fælles specifikationer for metadata, datastrukturer og sikkerhed.
- Nationale netværk med tilslutning af myndighedsløsninger, herunder selvbetjeningsportaler og registre som leverer OOTS-dokumentation.

I den danske kontekst består OOTS-netværket af to dele:

- Det danske netværk: Her tilslutter danske myndigheder sig og kommunikerer med Digitaliseringsstyrelsens OOTS-gateway (enten direkte eller indirekte via Blanketmotoren).
- Det europæiske netværk: Digitaliseringsstyrelsen videresender meddelelser til relevante access points i andre medlemslande.

Rollefordeling

Aktør	Rolle
Anmodende myndighed	Myndighed, som ønsker at hente dokumentation fra et andet EU-land
Udstedende myndighed	Myndighed som skal sende dokumentation til et andet lands myndighed.
Digitaliseringsstyrelsen (DIGST)	National gatewayoperatør – videresender meddelelser til/fra andre EU-medlemslande
Erhvervsstyrelsen (ERST)	Tilbyder blanketmotor som alternativ integrationsløsning (vs. direkte integration til OOTS-gateway)
EU Access Points	Modtager og besvarer anmodninger fra Danmark via deres respektive nationale systemer

Kommunikationsflow

Kommunikationsflowet for OOTS-meddelelser ser overordnet således ud:

- Den danske myndighed sender en anmodning via eDelivery gennem eget access point (fx en Domibus-instans) eller gennem Blanketmotorens indbyggede access point (ved indirekte integration). Meddelelsen modtages i Digitaliseringsstyrelsens OOTS-gateway (DKD).
- Meddelelsen valideres, logges og videresendes til det relevante EU-medlemslands access point.
- Det udenlandske access point sender svar tilbage til OOTS-gateway.
- DKD returnerer svaret til den danske myndighed.

Alle meddelelser sendes over AS4 og skal overholde de fælles specifikationer for OOTS, herunder sikkerhed, metadata og standardiserede datastrukturer.

Miljøer

Det danske netværk er opsat i to miljøer:

- Acceptance (Integrationstestmiljø): Anvendes til myndighedernes afprøvning
- Prod (Produktionsmiljø): Anvendes til real drift og er omfattet af særlige sikkerheds- og adgangskrav

Teknisk tilslutningsproces

Dette kapitel beskriver de tekniske trin, som en dansk myndighed (evt. med dennes IT-leverandør) skal gennemføre for at etablere integration med OOTS-gatewayen. Tilslutningen sker via eDelivery AS4-protokollen (Fx Domibus) og kan ske enten direkte fra myndighedens eget access point.

Overblik over tekniske forudsætninger

Før en myndighed kan påbegynde teknisk integration, skal følgende være på plads:

- Etablering af kontakt til Digitaliseringsstyrelsen (DIGST)
- Fastlæggelse af unikt *OOTS-registrerings ID*, som anvendes som OriginalSender

Udveksling af information

For at etablere forbindelse skal følgende oplysninger udveksles mellem Digitaliseringsstyrelsen og myndighedens tekniske kontakt:

Information fra myndighed	Information fra Digitaliseringsstyrelsen
Public certifikat (PEM-format)	Endpoints (test og produktion)
Oplysninger om AS4 Access Point: - PartyId - PartyName - URL	P-mode eksempler og skabeloner
Kontaktperson(er)	Tekniske kravspecifikationer
Oplysninger om myndighedsløsning: - Dansk SDG Procedure - EU SDG procedure - Selvbetjeningsløsning - Rolle (anmoder/udsteder)	Tilslutningsaftale til OOTS-gateway (DKD), se bilag 4)

Udvekslingen af oplysninger sker primært via myndighedens tilslutningsaftale med Digitaliseringsstyrelsen. Derudover skal foretages manuel udveksling og validering af certifikater, så TLS-kommunikationen kan etableres via Direct Trust.

Opsætning af P-mode

Myndigheden skal opsætte en P-mode-konfiguration, der matcher Digitaliseringsstyrelsen forventede format. Der skal være enighed om følgende parametre:

- PartyInfo.From/To (inkl. PartyId, Role og PartyIdType)
- Service og Action-kombinationer
- Legs og MEP (one-way)
- MessageProperties med originalSender, finalRecipient og trackingIdentifier
- Sammenhæng mellem certifikat-CN og PartyName

Digitaliseringsstyrelsen stiller skabeloner og eksempler til rådighed.

Firewall og netværksadgang

Myndighedens systemer skal kunne tilgå følgende endpoints via HTTPS (port 443):

Miljø	Endpoint URL	IP Adresse
Acceptance	https://oots-dk-ap-acc.digst.govcloud.dk/domibus/services/msh	188.64.157.49
Produktion	https://oots-dk-ap.digst.govcloud.dk/domibus/services/msh	TBA

Det anbefales at validere adgang via test-setup, inden beskeder forsøges afsendt.

Test og validering

Digitaliseringsstyrelsen anbefaler følgende fremgangsmåde til validering:

1. Afsend testbesked til acceptance-endpoint.
2. Verificer korrekt afsendelse i Domibus backend.
3. Kontroller at alle nødvendige AS4-headere er sat korrekt.
4. Digitaliseringsstyrelsen bekræfter modtagelse og struktur.
5. Eventuel test af end-to-end flow til EU-access point (fx Finland).

Ved succesfuld test gives grønt lys til produktionstilslutning.

Test og validering

Før en myndighed kan overgå til produktionsmiljøet, skal integrationen valideres i acceptancemiljøet. Testforløbet sikrer, at både tekniske og forretningsmæssige krav er opfyldt, og at myndighedens løsning kan indgå korrekt i det samlede OOTS-flow.

Formål med test

Testfasen har til formål at:

- Verificere at P-Mode-konfigurationen er korrekt opsat.
- Validere korrekt struktur og indhold af AS4-beskeder.
- Bekræfte at evidens kan sendes og modtages gennem OOTS-netværket.
- Sikre at tracking og routing fungerer korrekt via Digitaliseringsstyrelsen OOTS-gateway.
- Identificere tekniske eller semantiske fejl før produktion.

Krav til testmiljø

Myndighedens testmiljø skal:

- Kunne sende eDelivery AS4-beskeder til følgende endpoint: https://oots-dk-ap-acc.digst.govcloud.dk/domibus/services/msh
- Være konfigureret med relevante certifikater og Direct Trust
- Benytte det oplyste *OOTS-registrerings ID* som OriginalSender

Være i stand til at sende Evidence Requests og modtage Evidence Responses. Sidstnævnte bør teste mod Digitaliseringsstyrelsens OOTS Testprovider, inden testforløb påbegyndes.

Testforløb og samarbejde

Digitaliseringsstyrelsen tilrettelægger testforløbet i samarbejde med myndigheden og eventuelt ERST. Et typisk forløb:

- Forberedelse
- Udveksling af metadata og P-mode-parametre, upload af certifikater og forberedelse af testdata.
- Teknisk connectivity-test
- Bekræftelse af, at der kan etableres forbindelse og sendes beskeder til og fra Digitaliseringsstyrelsen.
- Validitet af AS4-beskeder
- Beskeder kontrolleres for korrekt headerstruktur, korrekt mapping af trackingIdentifier til PartyInfo.To.PartyId og gyldige dokumentformater.
- End-to-End test (E2E)

Myndigheden sender en Evidence Request via Digitaliseringsstyrelsens access point, som videresender til et EU-medlemslands access point (fx Finland). Myndigheden skal kunne modtage en korrekt struktureret Evidence Response.

Afslutning og godkendelse

Digitaliseringsstyrelsen validerer at alle krav er opfyldt, og myndigheden gives adgang til produktion.

Dokumentation og sporbarhed

Testaktiviteter dokumenteres og gemmes i tilfælde af senere revision eller behov for fejlfinding. Dette omfatter:

- Eksempler på request- og response-meddelelser.
- Logfiler fra Domibus.
- Skærmbilleder eller output fra backend.
- Valideringsrapporter og godkendelse fra Digitaliseringsstyrelsen.

Certifikater og sikkerhed

OOTS-beskeder overføres via AS4 og er underlagt høje krav til sikkerhed, integritet og autenticitet. Det danske OOTS-netværk benytter Direct Trust som tillidsmodel, hvilket betyder, at der ikke anvendes offentlige CA'er, men at parterne direkte udveksler og godkender hinandens certifikater.

Direct Trust-model

I Direct Trust-modellen:
Myndigheden sørger for egne certifikater, fx ved bestilling fra Statens-IT
Certifikater udveksles bilateralt og tilføjes lokalt i eDelivery Access Point som "trusted".

Der benyttes ikke CRL/OCSP, men tillid er baseret på manuel whitelisting
Fordelen er en høj grad af kontrol og uafhængighed – ulempen er større behov for koordination.

Certifikatkrav

Certifikater skal overholde følgende krav:

Parameter	Krav
Type	X.509 v3
Nøglelængde	Minimum 2048-bit RSA
Gyldighed	Skal være gyldigt i hele den forventede test-/driftsperiode
Anvendelse	Skal kunne anvendes til signering og kryptering
Fingerprint/SHA	Skal være kendt og udvekslet med Digitaliseringsstyrelsen
Udsteder	Statens-IT eller anden anerkendt CA

Der må ikke anvendes wildcard-certifikater.

Upload og administration i Domibus

Certifikater håndteres i Domibus på følgende måde:

- Offentlige certifikater fra modparten uploades til Truststore.
- Domibus konfigureres til at anvende korrekt certifikat for hvert P-Mode.
- Certifikater identificeres via Alias og knyttes til partnavne.

Sikkerhed i eDelivery AS4-protokollen

AS4-beskeder mellem myndighed og Digitaliseringsstyrelsen beskyttes med:

Sikkerhedsfunktion	Teknologi/anvendelse
Transport Layer Security	HTTPS med mutual TLS (Direct Trust)
Signatur	XML Digital Signature i AS4-headeren
Kryptering	XML Encryption af meddelelsens payload
Sikkerhedspolitik	Baseret på Domibus' BSP-standard (Basic Security Profile)

Typisk anvendes RSASSA-PSS til signatur og AES-256 til kryptering.

Certifikatrotation

Det anbefales at planlægge certifikatfornyelse i god tid.
Fremgangsmåde:

- Udarbejd nyt certifikat parallelt med det gamle
- Koordiner med Digitaliseringsstyrelsen om tidspunkt for rotation
- Upload nyt certifikat i god tid i både jeres og Digitaliseringsstyrelsen Domibus-installation
- Verificér at nyt certifikat virker ved testmeddelelse
- Fjern det gamle certifikat når skiftet er gennemført

Log-in til selvbetjeningsløsninger via Nemlog-in

Ved login med europæisk eID til selvbetjeningsløsninger, som er omfattet af krav om OOTS, implementeres login via NemLog-in med OIOSAML4.

Integration via Nemlog-in

Ved at sætte flueben for log-in med europæisk eID i myndighedens eksisterende integration til Nemlog-in, muliggøres at den enkelte selvbetjeningsløsning kan modtage eID fra udlandet. Myndigheder der implementerer OOTS skal dog udover at sætte flueben opgradere til OIOSAML 4.

OIOSAML 4

For at kunne understøtte modtagelsen af eIDAS-attributten "person.identifier", som anvendes ved anmodning om OOTS-dokumentation fra andre

medlemslande, skal myndigheden have opgraderet til OIOSAML 4. De øvrige eIDAS-attributter medsendes og modtages uden OIOSAML 4

Bemærk: Integration via Nemlog-in vil være tema for Digitaliseringsstyrelsens opgavepakke 4, og vil være relevant for alle myndigheder der er omfattet af både ATS (Adgang til selvbetjeningsløsninger) og OOTS-forpligtelserne. Ovenstående er dog særligt centralt for OOTS-omfattede myndigheder grundet behovet for attributten "person.identifier" og således behov for opgradering til OIOSAML 4.

Læs mere om OIOSAML her: https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

Læs mere om anvendelse af ikke-danske eID via Nemlog-in her: https://tu.nemlog-in.dk/oprettelse-og-administration-af-it-systemer/log-in#europaeiskeid

Teknisk tjekliste for myndigheder

Inden en tjeneste (anmodende selvbetjeningsløsning) indberettes til common services, skal følgende punkter som minimum fungere og være verificeret, inden tilslutning til OOTS-gateway påbegyndes.

- ☐ Integrér med **Evidence Broker** for mapping af evidencetyper på tværs af lande.
- ☐ Integrér med **Data Service Directory (DSD)** for at finde dokumentationsudstedere
- ☐ Brug **Semantic Repository** til at håndtere definitioner af datamodeller for standardiseret dokumentation
- ☐ Der skal sikres, at metadata, identifikatorer og sprog håndteres konsistent ved udveksling.
- ☐ Systemet skal kunne håndtere afsendelse af meddelelser, modtagelse af svar samt håndtere kvitteringer, fejl og retransmissioner via eDelivery-laget (signal lag).
- ☐ Bruger skal kunne viderestilles til preview eller login, hvis bevis-udsteder kræver det.
- ☐ Logning og fejlhåndtering, sporing af conversation identifiers osv. for fejlsøgning og audits bør være på plads.

Kontakt og support

For at sikre en smidig tilslutning og drift af OOTS-gatewayen stiller Digitaliseringsstyrelsen support og sparring til rådighed under hele processen – fra planlægning og test til produktion og videreudvikling.

Teknisk support
Ved tekniske spørgsmål, herunder P-mode-konfiguration, certifikatudveksling og AS4-beskedformater, kan følgende kontakt benyttes:

- E-mail: sdg@digst.dk
- Supportvindue: Hverdage 9:00–15:00 (CET)
- Svarfrist: Forventet svartid inden for 1–2 arbejdsdage

Vedhæft gerne følgende:

- Relevant P-mode-fil eller beskedlog
- Eksempel på request og/eller response
- Tidsstempel for afsendelse
- Eventuelle fejlbeskeder

Forretningsmæssige spørgsmål
Spørgsmål vedrørende kontraktuelle forhold, datatyper, tilslutningsaftaler eller ansvar i OOTS-rammen håndteres af:

- Digitaliseringsstyrelsens OOTS-team
- E-mail: sdg@digst.dk

Bilag

Bilagsliste

#	Titel	Format	Beskrivelse
3a, i)	Eksempel på P-Mode-konfiguration	XML	Indeholder alle nødvendige konfigurationselementer
3a, ii)	Request_response samples (zip)	XML	Brugbart til test og validering
3a, iii)	OpenPeppol eDEC Code Lists	Excel, GeneriCode, JSON, XML & HTML	https://docs.peppol.eu/edelivery/codelists/