**DIGITALISERINGSSTYRELSEN – edelivery**

**Pilot implementering af eDelivery - Rapport**

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

.

|  |  |
| --- | --- |
| **Version:** | 1.0 |
| **Status:** | Endelig |
| **Forfatter:** | Netcompany |



**Dokumenthistorik**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Dato | Forfatter | Status | Bemærkninger |
| 1.0 | 20-12-2019 | Netcompany | Endelig | Slutprodukt fra eDelivery pilot projekt |

**Referencer**

|  |  |  |  |
| --- | --- | --- | --- |
| Reference | Titel | Forfatter | Version |
| **[Domibus]** | <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus> | CEFDIGITAL | **2019-12-20** |
| **[SMP]** | <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP> | CEFDIGITAL | **2019-12-20** |
| **[Docker]** | <https://success.docker.com/article/maintenance-lifecycle> | Docker | **2019-12-20** |

Indholdsfortegnelse

[1 Introduktion 3](#_Toc27719501)

[1.1 Oversigt over slutprodukter 3](#_Toc27719502)

[2 eDelivery nøgle koncepter 3](#_Toc27719503)

[2.1 Access Point (AP) 4](#_Toc27719504)

[2.2 Service Metadata Publisher (SMP) 4](#_Toc27719505)

[2.3 Service Metadata Locator (SML) 4](#_Toc27719506)

[2.4 Oprettelse af Nyt AP og kommunikation imellem to AP’er 4](#_Toc27719507)

[3 Aktiviteter i pilot implementering 5](#_Toc27719508)

[3.1 Registrering af SMP domæne i Test-SML 5](#_Toc27719509)

[3.2 Registrering af AP i Test-SML 6](#_Toc27719510)

[3.3 Send besked med eDelivery 7](#_Toc27719511)

[4 Valg af software 7](#_Toc27719512)

[4.1 Valg af AP (Domibus) 7](#_Toc27719513)

[4.2 Valg af SMP (CEF SMP) 7](#_Toc27719514)

[4.3 Valg af container løsning (Docker) 8](#_Toc27719515)

[5 Udfordringer i forbindelser med pilotprojektets valg 8](#_Toc27719516)

# Introduktion

I november og december 2019 er der over fem uger kørt et pilotprojekt for opsætning af et testmiljø for et eDelivery netværk i Danmark. Denne rapport giver en kort introduktion til eDelivery komponenterne samt de aktiviteter der er gennemført i pilotprojektet.

## Oversigt over slutprodukter

Som en del af projektet er der udarbejdet følgende slutprodukter

|  |  |  |
| --- | --- | --- |
| Navn | Link | Beskrivelse |
| Dokumenter | | |
| Pilot implementering af eDelivery - Rapport | [Link](https://goto.netcompany.com/cases/GTE610/DIGEDEL/Deliverables/Pilot%20implementering%20af%20eDelivery%20-%20Rapport.docx) | Et overblik over eDelivery som koncept og Netcompanys pilot implementering. |
| C0200 – User manual for administration AP and SMP | [Link](https://goto.netcompany.com/cases/GTE610/DIGEDEL/Deliverables/C0200%20-%20User%20manual%20for%20Administrating%20the%20AP%20and%20SMP.docx) | En bruger manual der beskriver administrationen af en Service Metadata Publisher (SMP) og et Access Point (AP). Denne er tiltænkt administratorer i f.eks. Digitaliseringsstyrelsen. |
| CO0200 – User manual for new Access Points | [Link](https://goto.netcompany.com/cases/GTE610/DIGEDEL/Deliverables/C0200%20-%20User%20manual%20for%20new%20Access%20Points.docx) | En bruger manual der beskriver administrationen et enkelt Access Point (AP). Denne er tiltænkt en ekstern part der ønsker at opsætte en AP og teste adgang til test-netværket. |
| O0100 – Installation guide | [Link](https://goto.netcompany.com/cases/GTE610/DIGEDEL/Deliverables/O0100%20-%20Installation%20Guide.docx) | Installations guide det giver en detaljeret beskrivelse af installationen a AP & SMP i Docker, Samt beskriver opsætningen af AP’et & SMP’en for at kunne teste forbindelsen. |
| 00400 – Technical Infrastructure | [Link](https://goto.netcompany.com/cases/GTE610/DIGEDEL/Deliverables/O0400%20-%20Technical%20Infrastructure.docx) | Beskrivelse af den tekniske infrastruktur for test miljøet. |
| Driftsmodning af eDelivery – overordnet roadmap | [Link](https://goto.netcompany.com/cases/GTE610/DIGEDEL/Deliverables/Driftsmodning%20af%20eDelivery%20-%20Overordnet%20roadmap.docx) | Et roadmap der i overordnede trin giver et bud på de problemstillinger og opgaver der skal løses før en dansk eDelivery løsning er driftsmoden. |
| Teknisk opsætning | | |
| Test miljø med AP & SMP | [SMP](http://212.98.96.26/ui/#/login?returnUrl=%2Fdomain) [AP](http://212.98.96.26:8080/domibus/) | Installation af CEF SMP og Domibus AP. Inkl. 12 måneders drift. De to links er til henholdsvis den opsatte CEF SMP og det forbundne Domibus AP. |
| Kode til opsætning af AP & SMP i Docker | [Link](https://goto.netcompany.com/cases/GTE610/DIGEDEL/Deliverables/edelivery%20-%20code.zip) | En zip fil, der indeholder koden til at opsætte et AP eller en SMP skal i en Docker container. |

# eDelivery nøgle koncepter

eDelivery netværket består af tre grundkomponenter, et Access Point (AP), en Service Metadata Publisher (SMP) og en Service Metadata Locator (SML).

Konfiguration af SML’en er ikke en del af pilotprojektet da den er stillet til rådighed og vedligeholdt af Connecting Europe Facility (CEF). I dette pilotprojekt er der i stedet forbundet til den officielle acceptance-test udgave af SML kaldet SMK.

De følgende afsnit beskriver komponenterne.

## Access Point (AP)

Hvert AP er en afsender eller modtager i eDelivery netværket. Fra et AP at der bliver sendt og modtaget data fra andre AP’er via AS4 protokollen. En slutbruger sender ikke beskeder direkte fra et access punkt, men i stedet videreformidler AP’et beskeder fra et kildesystem der integrerer til et AP. F.eks. kunne en dansk region have ét fælles Access Punkt, som de enkelte sygehuse afsender beskeder vha.

## Service Metadata Publisher (SMP)

I eDelivery er det SMP’en der udstiller data på alle dets tilhørende AP’er. SMP’en indeholder metadata for alle de individuelle AP’er og holde den centrale SML opdateret om hvilken SMP hver AP er tilknyttet. Metadata indeholder al den information der er nødvendig for at en anden part kan afsende en meddelelse, f.eks. endpoint adresse, AP-certifikat til kryptering og beskrivelse af hvilke formater der modtages.

Et eksternt AP kan så forespørge om opdateret information om en slutmodtager baseret på f.eks. et CVR-nummer. Det kunne f.eks. være en region hvis en journal skal sendes om en patient.

## Service Metadata Locator (SML)

I SML’en registreres alle services på AP’er i eDelivery. Dette sker via den SMP som et AP er tilknyttet og SML’en opdaterer derefter det globale DNS netværke så hver service i de tilknyttede AP’er peger tilbage til den korrekte SMP hvor afsendere kan hente metadata for servicen. Dette betyder at eDeliverys normale drift er uafhængig af SML’en da denne kun bruges til at opdatere DNS systemet.

## Oprettelse af Nyt AP og kommunikation imellem to AP’er

Oprettelse af et nyt AP eller opdatering af services på et eksisterende AP er visualiseret i Figur 1.

Et nyt AP bliver oprettet hos SMP’en og SMP’en registrerer disse i SML’en som opdaterer DNS netværket. Andre AP’er kan nu fremsøge information via den tilhørende SMP.



Figur oprettelse eller opdatering af et AP

Figur 2 illustrerer en afsendelse af en meddelelse via eDelivery. Som det ses indgår SML’en ikke i dette flow, da denne blot har opdateret DNS’en.



Figur Send besked fra via et AP til en modtager.

1. Et afsender system sender en besked til et afsender AP det integrerer til.
2. Afsender AP’et forespørger derefter DNS’en ud fra modtaget navnet. Dette returnerer adressen på den korrekte SMP.
3. Derefter kontaktes SMP’en for at modtage metadata, certifikater og adressen på modtager AP’et.
4. Afsender AP’et kan nu sende den egentlige besked via AS4 protokollen som er krypteret på baggrund af modtager certifikatet.
5. Beskeden ligger nu hos modtaget AP’et og modtagersystemet kan hente beskeden herfra.

# Aktiviteter i pilot implementering

I dette pilotprojekt er der blevet opsat et Access Points med Domibus og en SMP med CEF’s SMP software. Begge applikationer er tilgængelige i et i testmiljø. Desuden er der opsat et lokalt AP til at teste afsendelse til testmiljøet.

Den opsatte SMP er udstyret med en trust- og keystore til henholdsvis verificering af AP’er og SMP’ens egen privatnøgle. Den nuværende opsætning benytter et EU test certifikat til SMP’en som er stillet til rådighed af CEF eftersom den europæiske SML ikke understøtter danske (OCES) certifikater før februar 2020.

I pilotprojektet er der gennemført nedenstående tre test-scenarier. Disse svarer til de officielle steps i [eDelivery Connectivity testing](https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Connectivity+testing) dog uden denne formelt er gennemført.

## Registrering af SMP domæne i Test-SML

Registrering af et nyt SMP-domæne i SML’en er en manuel proces der foretages i samarbejde med CEF. I pilot projektet er den opsatte test SMP registreret i CEF’s acceptance test udgave af SML’en. Test udgaven af SML kaldes også SMK.

For at kunne registrere et SMP domæne på SMK skal SMP’en oprettes af CEF og der udveksles certifikater. Pilotprojektet har vist at CEF desværre ikke understøtter de danske OCES-certifikater. Den tekniske årsag er at OCES benytter sig at ”multi-value-RDN”, som er en del af certifikat standarden som CEF fejlagtigt ikke understøtter

For at arbejde uden om dette har vi i pilotprojektet registreret vores SMP ved brug af et test certifikat udsted af CEF selv. Dette bør ændres som en del af driftsmodningen af test miljøet. Iflg. CEF understøttes dette fra slut februar 2020.

## Registrering af AP i Test-SML

Efter registrering af SMP hos CEF kan SMP’en via web-service registrere og af-registrere AP’er i SML. I pilotprojektet er test SMP’en og tilhørende AP med én service registreret i SMK. DNS registreringen kan findes på [listen hos CEF](https://acc.edelivery.tech.ec.europa.eu/edelivery-sml/listDNS). Den danske SMP er navngivet dk.acc.edelivery.tech.ec.europa.eu.

I Figur 3 ses et overblik over oprettelse eller opdatering et AP i SML. SMP’en indeholder information for alle tilhørende AP’er såsom hvilken digitale adresse de befinder sig på, hvilket certifikat der tilhører dem, og hvilken metadata beskriver deres processer og dokumenter.



Figur – Registrering i SMK i pilotprojekt

## Send besked med eDelivery

I Figur 4 ses et overblik over de udførte handlinger i pilot projektet for at sende en besked vha. test SMP’en. Afsenderen laver et DNS lookup baseret på Modtager AP’s participant-id. Det giver afsenderen den tilknyttede SMP’s adresse, hvilket den bruger til at kontakte SMP’en og derigennem få fat i modtagerens metadata, såsom dens adresse og certifikat til kryptering. Så snart afsenderen har modtaget metadata kan den sende en besked via eDelivery og AS4 protokollen til modtageren.

I piloten foretages DNS opslaget i en lokal DNS fil der er opdateret med SMP IP-adressen. Dette skyldes udfordringer med opslag i den globale DNS efter registrering i SMK.



Figur – Afsendelse af besked i pilot projekt

# Valg af software

Herunder følger de valg der er blevet taget i pilot projektet i forhold til valg af software og implementeringsplatform.

## Valg af AP (Domibus)

Det opsatte AP’et er en installation af open source softwaren Domibus. Domibus (Domain Interoperability Bus) er en eDelivery AS4 overensstemmende Access Point implementering vedligeholdt af CEF Digital. Domibus softwaren er open source og til fri afbenyttelse kommercielt. Der bliver løbende frigivet nye Domibus releases, der bliver gratis fra CEF supporteret i en periode på omkring to år. Versionen brugt i dette pilotprojekt er v4.1.2 der er understøttet indtil 29.11.2021.

I pilot projektet løsningen er der valgt at bruge en installation med *Apache Tomcat* som Java server og *MySQL* som database eftersom CEF har udgivet en opsætning med netop denne kombination. Begge komponenter er bredt anvendte standard open source komponenter.

Domibus har fuld understøttelse af AS4 og eDelivery kører i produktion i flere sammenhænge, og er derfor muligt at køre videre med en driftsmoden løsning. Administration og brug af Domibus er veldokumenter fra CEFs side, og der bl.a. konfigurationseksempler tilgængelige for at sende test beskeder.

## Valg af SMP (CEF SMP)

De samme kendetegn gør sig gældende for den valgte SMP løsning. Den er ligeledes open source og vedligeholdt af CEF Digital. Den benyttede SMP version er v4.1.1 der blev udgivet i 10.10.2019 og er understøttet indtil: 10.10.2020.

Opsætningen er lavet på samme konfiguration og benytter sig også af *Tomcat* og *MySQL*.

## Valg af container løsning (Docker)

Løsningen er baseret den af de mest anvendte container-løsninger i industrien Docker. Både SMP’en og Test-AP’en er installeret via Docker for at sikre platformsuafhængighed for løsningen. Docker sørger samtidig for at hente det nødvendige software for systemet såsom Tomcat og MySQL, sådan at systemet også nemt kan startes op.

# Udfordringer i pilotprojektet

Udover normalt forventede opgaver med konfiguration og opsætning er standardprodukter, er der belyst nogle udfordringer i forbindelse med pilotprojektet som man bør være opmærksom på i det videre arbejde.

Det primære opmærksomhedspunkt er den manglende understøttelse af OCES certifikater i CEF’s infrastruktur. Dette har vi gjort dem opmærksom på i forbindelse med detteprojekt, og CEF forventer det løst i Marts 2020.

Dette medfører blandt andet at den nuværende opsætning anvender et test-certifikat udleveret af CEF til både SMP’en og AP’erne. I en egentlig drift opsætning af eDelivery i dansk kontekst skal de nuværende certifikaterne udskiftes danske OCES certifikater og funktionaliteten gentestes med anvendelse af disse. Problemet med OCES certifikater opstår både ved registrering i SML/SMK men også ved indlæsning af disse i SMP keystore hvor de lige nu valideres som ugyldige.

Indlæsning af certifikater har generelt været en udfordring i pilotprojektet eftersom standard-softwaren (SMP og Domibus) ikke vil starte op i Docker hvis certifikaterne ikke kan anvendes. Dette problem er dog løst i den Docker opsætningen som leveres som en del af pilotprojektet, men vil kan problemer igen hvis komponenterne skal konfigureres på ny.