Rollekataloget

Løsningsbeskrivelse

**Date**: 28.02.2017

**Author**: BSG

Indholdsfortegnelse

[1 Indledning 3](#_Toc494800338)

[1.1 Højniveau beskrivelse af løsningen 3](#_Toc494800339)

[2 Løsningsbeskrivelse 3](#_Toc494800340)

[2.1 Brugergrænseflade funktionalitet 4](#_Toc494800341)

[2.1.1 Login til brugergrænsefladen 4](#_Toc494800342)

[2.1.2 Administration og modellering af roller 4](#_Toc494800343)

[2.1.3 Tildeling af roller til brugere 6](#_Toc494800344)

[2.1.4 Understøttede dataafgrænsningstyper 7](#_Toc494800345)

[2.2 API til bruger-opslag 8](#_Toc494800346)

[2.3 Read-only API 8](#_Toc494800347)

[2.4 API til rolle-tildeling 8](#_Toc494800348)

[2.5 AD FS integration 8](#_Toc494800349)

[2.6 API til indlæsning af Organisationsdata 8](#_Toc494800350)

[2.7 Kendte begrænsninger 8](#_Toc494800351)

[2.8 Teknisk design 9](#_Toc494800352)

[3 Leverancebeskrivelse 9](#_Toc494800353)

[4 Tidsplan 9](#_Toc494800354)

**Historik**

28.02.2017 Opdateret efter præsentation af løsning i Hinnerup. API til at vedligeholde rolletildelinger tilføjet. DB læseadgang tilføjet. Understøttelse af tekst-værdier til dataafgrænsningsværdier. AD FS attribute store mere detaljeret beskrevet.

# Indledning

I forbindelse med kommunernes integration til støttesystemet Adgangsstyring for brugere, er kommunerne pålagt opgaven at vedligeholde et lokalt rolle/rettighedskatalog lokalt, og vedligeholde hvilke medarbejdere der har hvilke roller.

Dette dokument beskriver en teknisk løsning, der både kan favne den opgave som er nødvendig for at anvende de monopolbrudssystemer der kommer fra KOMBIT, men også kan finde anvendelse til andre systemer der anvender en rolle-baseret sikkerhedsmodel.

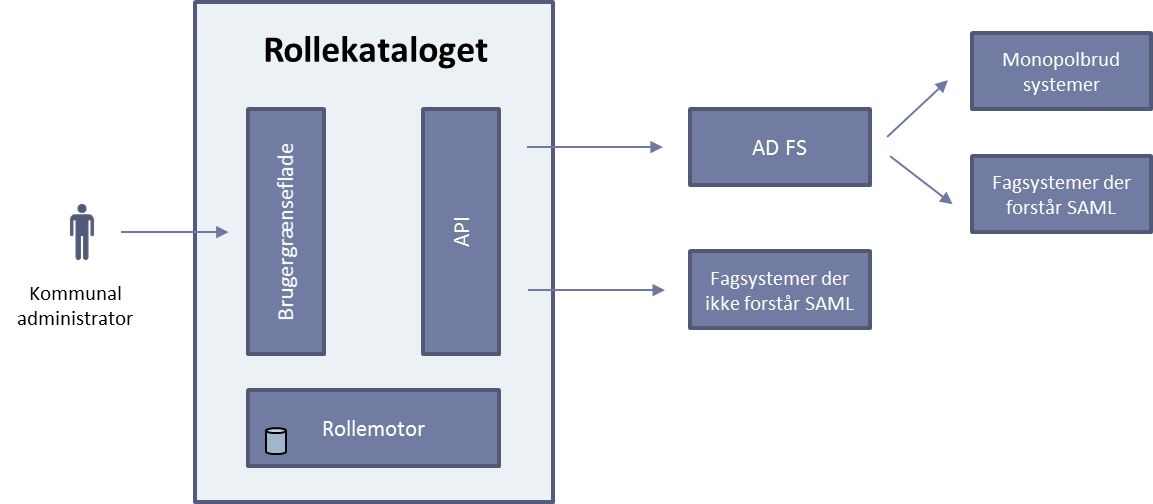
## Højniveau beskrivelse af løsningen

Den løsning der beskrives i dette dokument, består i grove træk af en web-baseret brugergrænseflade til at administrere rollerne i rollekataloget, samt en service-snitflade til at lave opslag på enkelt-brugere, for at få brugerens tildelte roller.

Løsningen kan driftes lokalt i kommunen, men tilbydes også en som Software-as-a-Service (SaaS) løsning, som driftes, overvåges, supporteres og vedligeholdes af Digital Identity.

Løsningen indeholder en integration til Active Directory Federation Services (AD FS), så den kan anvendes til at udstede SAML tokens til de fagsystemer der understøtter single-signon med SAML – dette dækker bl.a. de KOMBIT-leverede monopolbrudsystemer.

Fagsystemer der ønsker at trække brugernes rettigheder direkte ud af rollekataloget, kan gøre dette ved at bruge den snitflade der udstilles til formålet.



Figur 1 - systemoverblik

# Løsningsbeskrivelse

Den samlede løsning består af en række del-komponenter, som er beskrevet i detaljer nedenfor.

## Brugergrænseflade funktionalitet

Brugergrænsefladen er web-baseret, og er optimeret til moderne web-browsere, dvs Internet Explorer 9 og højere, samt Chrome, Firefox og lignende moderne web-browsere. Brugergrænsefladen er ikke optimeret til anvendelse på små skærme (smartphones og lignende), men kan dog fungere på disse.

Løsningen er baseret på et Bootstrap theme kaldet ’Angle’[[1]](#footnote-1), der kræver køb af en 1-gangs licens på $18 for at anvende. Digital Identity har en site-licens til at anvende Angle til alle egen-hostede løsninger, og det er kun nødvendigt at købe en licens hvis man ønsker at drifte løsningen selv.

### Login til brugergrænsefladen

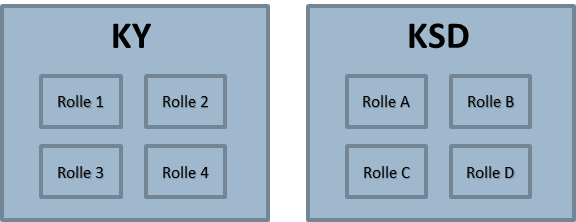
Login til Rollekataloget håndteres via SAML single-signon, og kommunen kan fx anvende sin eksisterende AD FS opsætning til at håndtere login til Rollekataloget.

Når man er tildelt adgang til Rollekatalogets brugergrænseflade, kan man tilgå alt funktionaliteten i Rollekataloget.

### Administration og modellering af roller

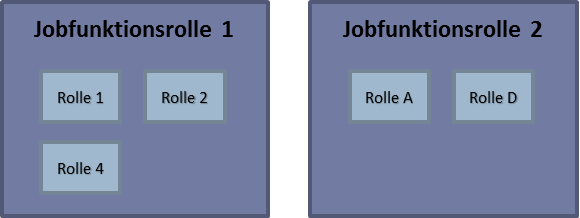
Rollekataloget håndterer 3 niveauer af roller

* **Brugersystemroller**. Disse roller er ejet af det enkelte fagsystem, og udstilles som byggeklodser i brugergrænsefladen. Man kan ikke ændre i disse roller, da de er ejet af det fagsystem de kommer fra.



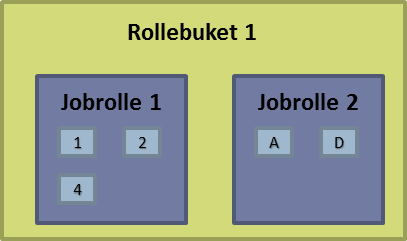
Figur 2 – Brugersystemroller, ejet af fagsystemerne

* **Jobfunktionsroller**. Disse roller bygges af Brugersystemroller, og er myndigheds-specifikke. Til disse roller er det muligt at knytte dataafgrænsninger jf KOMBITs rettighedsmodel. Disse roller er bundet til ét bestemt it-system, og det er dermed ikke muligt at bygge en Jobfunktionsrolle der indeholder Brugersystemroller fra forskellige fagsystemer (til dette formål anvendes Rollebuketter).



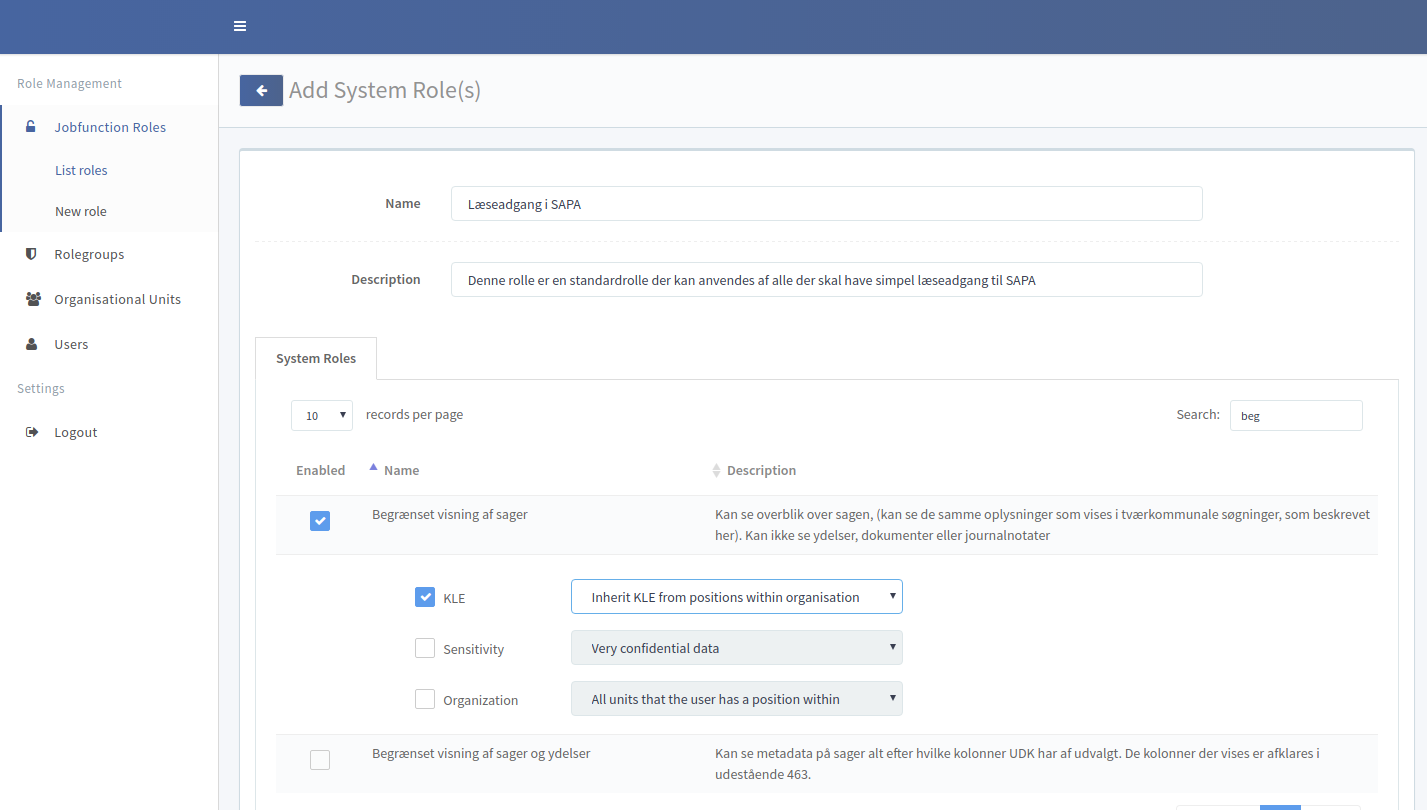
Figur 3 – Jobfunktionsroller, indeholdende Brugersystemroller

* **Rollebuketter**. Rollebuketter er en nem måde at gruppere Jobfunktionsroller, så man fx kan opbygge en rolle der dækker over flere it-systemer.

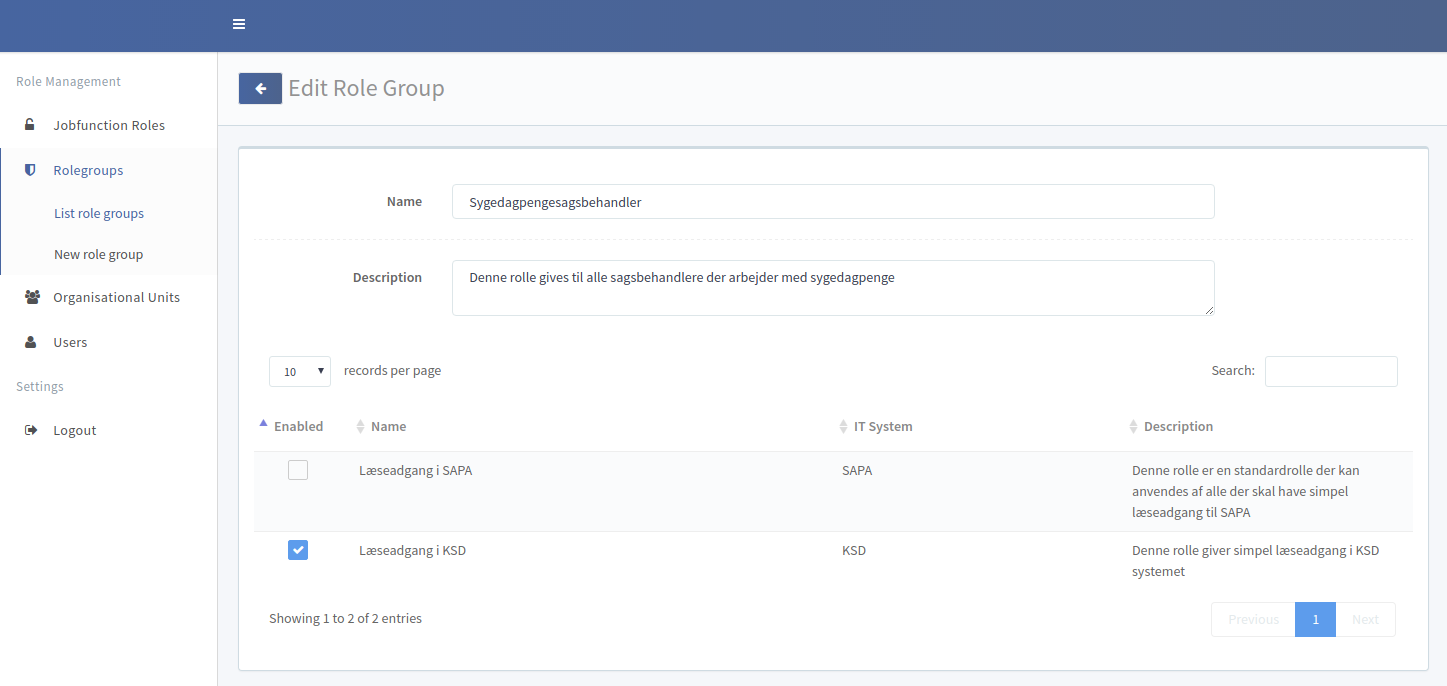


Figur 4 – Rollebuket indeholdende Jobfunktionsroller

Nedenfor er vist skærmbilleder der viser hvordan man arbejder med hhv Jobfunktionsroller og Rollebuketter.



Figur 5 – modellering af en Jobfunktionsrolle



Figur 6 – modellering af en Rollebuket

### Tildeling af roller til brugere

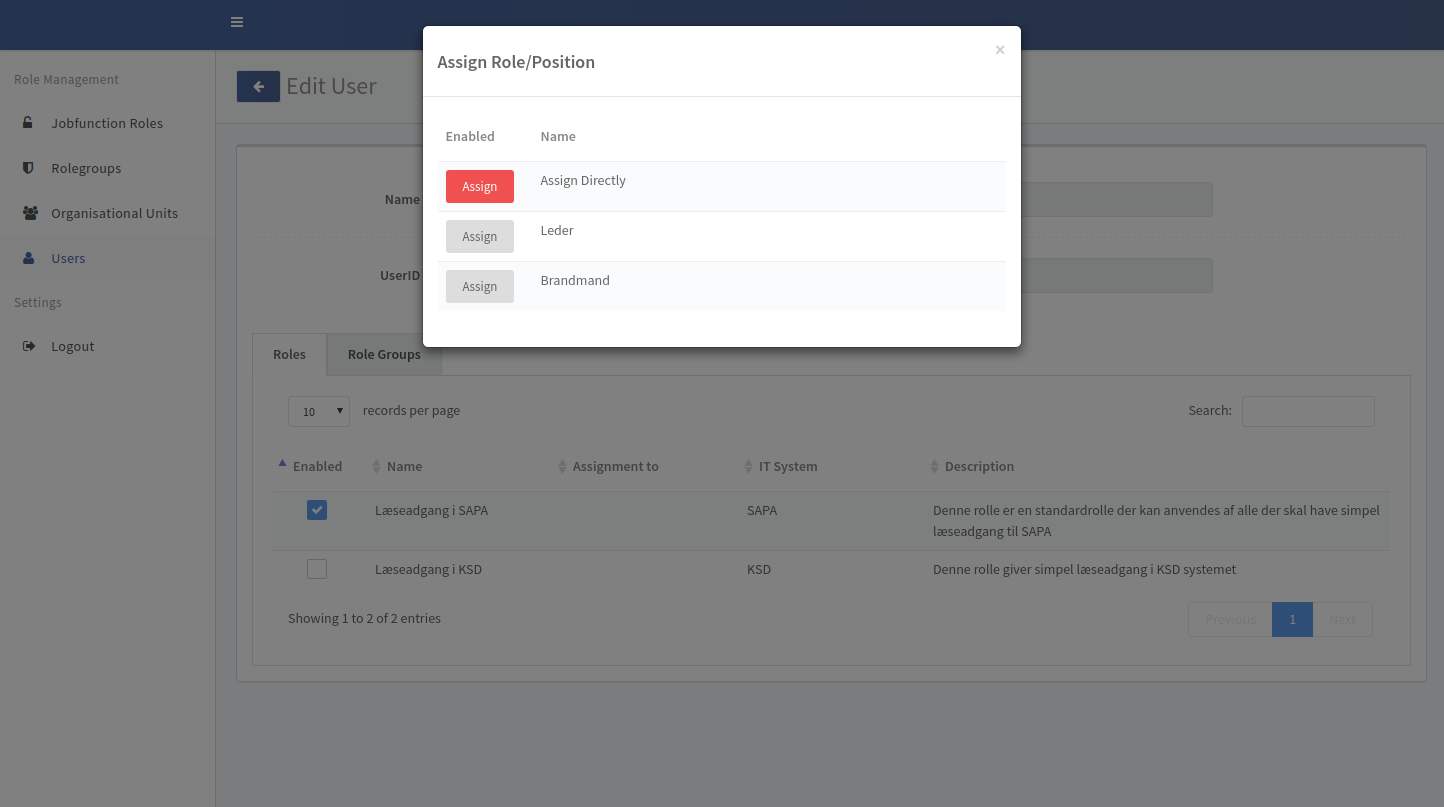
Når der tales om tildeling af roller, så kan der både være tale om tildeling af en Jobfunktionsrolle samt tildeling af en Rollebuket. Hvis man tildeler en Rollebuket, er denne tildeling dynamisk, på den måde forstået at hvis buketten ændrer indeholder (fx hvis der tilføjes en ekstra Jobfunktionsrolle til buketten), så slår denne ændring igennem på alle der har denne buket tildelt.

I nedenstående omtales Jobfunktionsroller og Rollebuketter under fællesbegrebet ”roller”, og den nævnte funktionalitet gælder for begge typer af roller.

Tildelingen af roller til en bruger kan ske på flere niveauer.

* **Tildeling via enhed**. I brugergrænsefladen kan man tildele en rolle til en enhed. Når man tildeler en rolle til en enhed, betyder det at alle brugere der har et ansættelsesforhold (stilling) i denne enhed automatisk tildeles denne rolle. Hvis rollen fjernes fra enheden, så fjernes den også automatisk fra alle medarbejdere i denne enhed. Ligeledes hvis en medarbejder ophører med at arbejde i enheden, så fjernes rollen også automatisk.
* **Tildeling via stilling**. I brugergrænsefladen kan man også tildele en rolle til en brugers stilling i en given enhed. Det betyder at brugeren har denne rolle så længe brugeren har denne stilling. Hvis brugeren mister stillingen, så fjernes rollen automatisk fra brugeren.
* **Tildeling direkte til brugeren**. I brugergrænsefladen kan man også tildele en rolle direkte til en bruger. I dette tilfælde er der ingen automatik der fjerner rollen igen, og når brugeren ikke længer skal have denne adgang, skal man huske at fjerne rollen fra brugeren igen.

Nedenfor er vist et eksempel på rolle-tildeling på en bruger, hvor man kan knytte rollen til brugerens stilling.



Figur 7 – tildeling af rolle knyttes til bestemt ansættelsesforhold

### Understøttede dataafgrænsningstyper

Brugergrænsefladen har optimerede UI komponenter til de fælleskommunale dataafgrænsningstyper KLE, OrganisationEnhed og Følsomhed. For andre dataafgrænsningstyper understøttes alene tekst-indtastning.

## API til bruger-opslag

Der udstilles et API til at slå op hvilke roller en bruger er tildelt, API’et tager et bruger-id og et it-system som input, hvorefter den svarer med en JSON struktur, der indeholder de roller som brugeren er tildelt til netop dette it-system.

Svaret indeholder også en OIO-BPP enkodet struktur, der kan sendes til de fagsystemer der understøtter OIO-BPP.

Svaret indeholder også en korrekt formateret NameID/Subject, der kan anvendes af AD FS til at udstede et rammearkitektur-kompatibelt token.

## Read-only API

Rollekataloget udstiller følgende data i systemet via et read-only API, som kan anvendes til forskellige formål, herunder rapportering m.m.

* List alle Jobfunktionsroller
* List alle Rollebuketter
* List alle roller tildelt en medarbejder
* List alle roller tildelt en enhed
* List alle medarbejdere der er tildelt en bestemt rolle (enten direkte eller indirekte via organisatorisk indplacering)

## API til rolle-tildeling

Der udstilles et API til at fjernstyre rolletildelinger, dvs følgende operationer

* Tildel/fjern rolle til medarbejder
* Tildel/fjern rolle til enhed

Bemærk at man kan bruge read-only API’et til at trække stamdata ud om roller, så man kan anvende disse som input til rolle-tildeling.

## AD FS integration

Sammen med Rollekataloget medfølger et såkaldt *Custom Attribute Store* til AD FS, der kan kalde Rollekataloget og udstiller et KOMBIT-kompatibelt SAML token på baggrund af dette opslag.

## API til indlæsning af Organisationsdata

Da støttesystemet Organisation lader vente på sig, understøtter Rollekataloget at man kan indlæse sine Organisatoriske data (enheder og medarbejdere, samt KLE opmærkning af enhederne) via et API, der tager en fuld organisation i JSON format.

Når støttesystemet Organisation er klar, er Rollekataloget forberedt til at kunne læse data derfra i stedet for at indlæse data via dette API.

## Kendte begrænsninger

* Der er ingen brugergrænseflade til at vedligeholde fagsystemers og deres brugersystemroller. Disse indlæses på nuværende tidspunkt i databasen via et SQL script.
* Der er ingen integration til støttesystemet Administrationsmodul, så de Jobfunktionsroller man opbygger i Rollekataloget skal også oprettes i støttesystemet Administrationsmodulet. KOMBIT planlægger dog at udstille et API på støttesystemet Administrationsmodulet, så på sigt bliver det muligt at automatisk oprette data i støttesystemet, uden at man skal oprette dem manuelt (dette er en videreudviklingsopgave).
* Der er ingen brugergrænseflade til at vedligeholde organisatoriske data (enheder og medarbejdere), disse vedligeholdes udenfor Rollekataloget, og indlæses via API’et til dette formål.

## Teknisk design

Løsningen udvikles i Java (Spring til backend, Thymeleaf til frontend og Hibernate til datalaget), og pakketeres som et Docker Image, klar til deployment i en Docker Host.

Som database anvendes MySQL under udviklingen, og Aurora til drift (det er også muligt at anvende MySQL til drift hvis man ønsker at drifte løsningen selv).

# Leverancebeskrivelse

Løsningen består af flere artefakter, som listet nedenfor

* Et Java kode-projekt med Rollekatalogets kildekode
* Et C# projekt med kildekoden til *Custom Attribute Storet* til AD FS
* En pre-kompileret udgave af *Custom Attribute Storet*, klar til deployment i AD FS 3.0 på en Windows Server 2012 R2, samt en tilsvarende udgave til AD FS 2.1 på en Windows Server 2012.
* En opdateret løsningsbeskrivelse (dette dokument)
* En brugervejledning
* Teknisk dokumentation til drift og videreudvikling
* Teknisk dokumentation af API’erne med eksempel data

# Tidsplan

Løsningen sættes i pilot-drift med Favrskov Kommune som pilot medio marts, for at understøtte deres ibrugtagning af Tricom eCommerce.

I pilotperioden er SLA’erne for driften ikke gældende, da der kan være flere servicevinduder, tilpasninger m.m. end SLA’erne normalt tillader.

Løsningen forventes at være fuldt tilgængelig, i normal drift, for alle tilsluttede kommuner maj 2017.

1. <https://wrapbootstrap.com/theme/angle-bootstrap-admin-template-WB04HF123> [↑](#footnote-ref-1)