

# SP Link tilslutningsvejledning

## Indhold

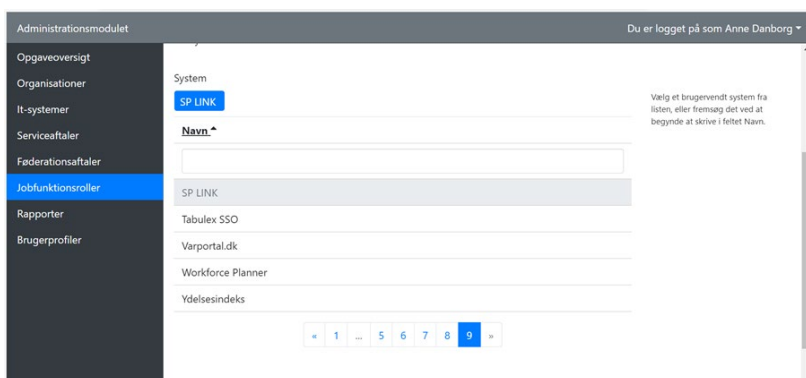
Introduktion.....	1
Systemlandskab.....	2
Tilgængelig miljøer .....	3
Sikkerhed .....	4
Krav til brugere .....	4
Brug af SPLIFE .....	4
Opsætning i Cura .....	5
Logning .....	6

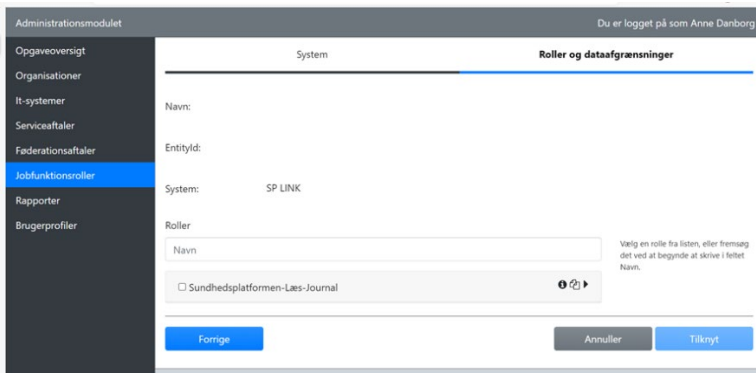
## Introduktion

Dette dokument beskriver SPLIFE (**SP Link Frontend**) som muliggør kommuners slutning til SP Link, og dermed kommunale brugeres adgang til patientjournaler i Sundhedsplatformen uden at kommunen behøver at oprette SP Link brugerkonti til alle de brugere som skulle have adgang til patientjournaler.

Kommunerne slutter sig til SP Link ved at registrere deres IdP med Kombit Context Handler og oprette en Jobfunktionsrolle.

1. Kommunens STS administrator på Serviceplatformen skal oprette SP-link i Kombit og tildele **Jobfunktionsrolle** som er knyttet til Brugersystemrolle **Sundhedsplatformen-Læs-Journal** i **Administrationsmodulet**
2. Kender man ikke navnet på Kommunens STS systemadministrator kan man få det oplyst på [kdi@kombit.dk](mailto:kdi@kombit.dk)



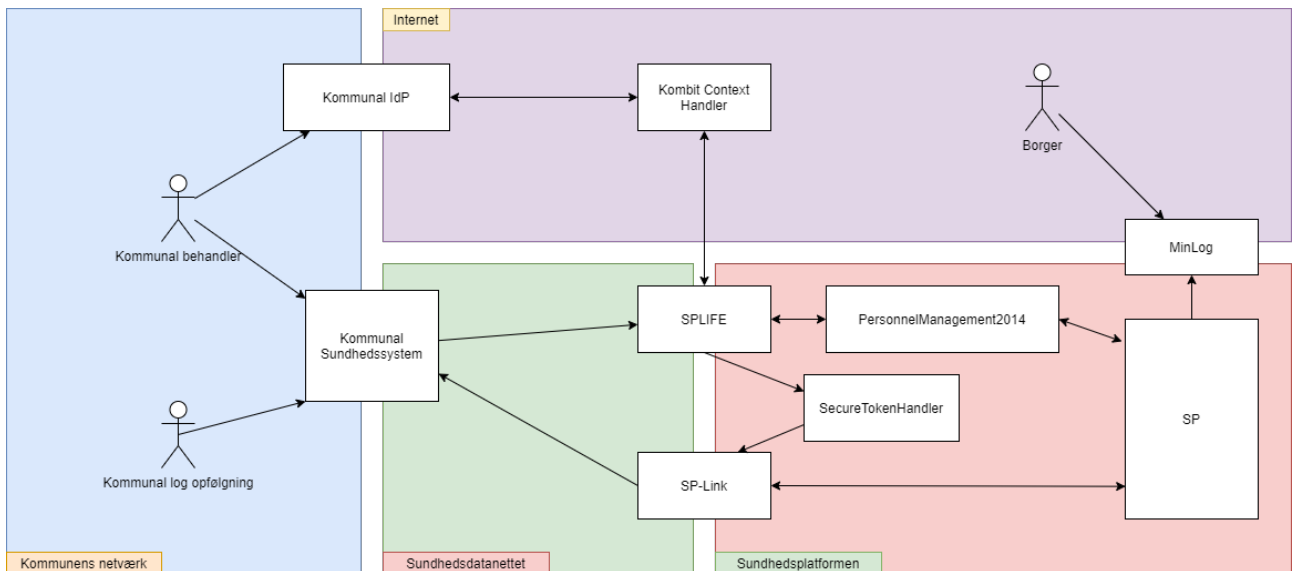


De kommunale brugere får begrænset adgang til patientjournaler direkte fra de kommunale sundhedssystemer via deeplinks. Kombit Context Handler autentikerer den kommunale bruger mod SPLIFE, og SPLIFE sørger for autentificering mod SP Link.

Hvis kommunen er sluttet til SP Link (gennem SPLIFE), og brugeren har den korrekte rolle tildelt, vil brugeren ved at klikke på en deeplink få vist en patientjournal. Brugeren får adgang til en patientjournal ad gangen. Hver patientjournal kræver sit eget deeplink, og hvert deeplink giver adgang til en specifik patientjournal. Brugeren kan ikke skifte patient uden at klikke på et nyt deeplink. Hvis brugeren klikker på et nyt deeplink mens de stadig har en patientjournal åben bliver de automatisk logget ud fra foregående patientjournal.

## Systemlandskab

Figur 1 beskriver hvordan de involverede systemers relation til hinanden. Al kommunikation sker med HTTPS over port 443.



Figur 1: Systemlandskab

De kommunale sundhedssystemer tilgår SPLIFE gennem Sundhedsdatanettet. SPLIFE kan ikke tilgås udenfor Sundhedsdatanettet. Kommunale brugere tilgår patientjournaler via deeplinks som kommunerne opretter på deres egne sundhedssystemer. Brugere får adgang hvis de er logget på hos deres egen IdP. Uden gyldig

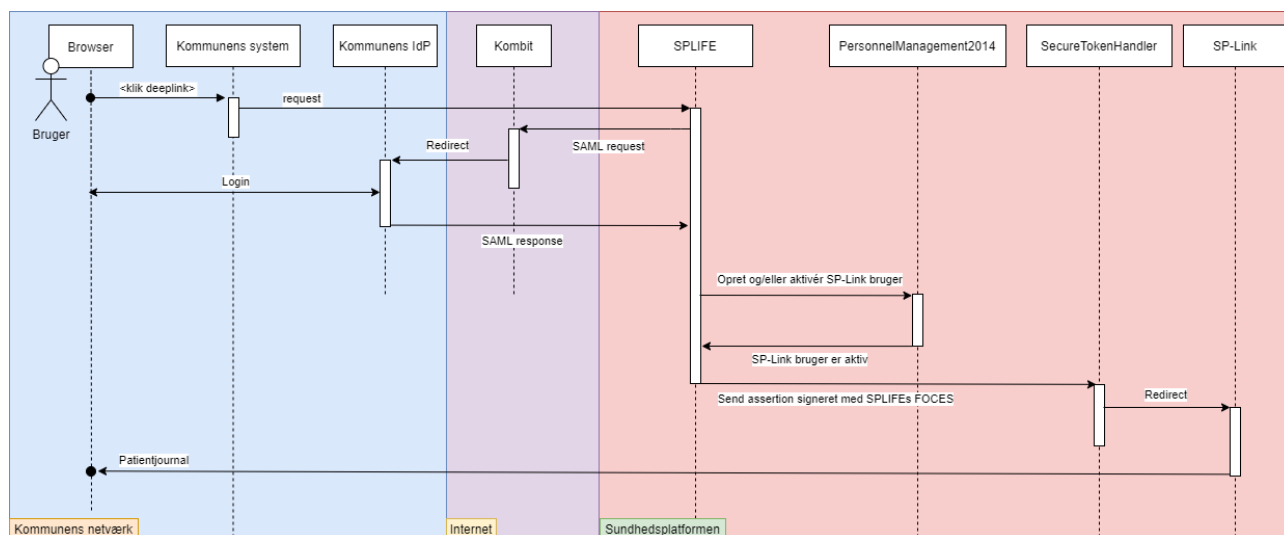
login session vil kommunale brugere omdirigeres til deres normale login side. Med en gyldig login session, og den påkrævede rolle Sundhedsplatformen-Læs-Journal, vil brugere få den anmodet patientjournal vist i deres browser. Brugeren bliver logget ud af patientjournal automatisk efter 15 minutters inaktivitet, eller hvis brugeren klikker på et andet deeplink. Kun en patientjournal per bruger vises ad gangen.

SPLIFE kender ikke til de kommunale IdP'er, Kombit Context Handler sørger for at SAML requests og responses bliver omdirigeret mellem SPLIFE og IdP. SPLIFE stoler på at de brugere som har adgang til Sundhedsdatanettet, og som Kombit Context Handler autentikerer, og som har den påkrævede rolle Sundhedsplatformen-Læs-Journal kan gives adgang til den anmodede patientjournal.

For at få adgang til patientjournaler opretter SPLIFE en systembruger på Sundhedsplatformen. Denne bruger kan ikke tilgås uden SPLIFE. SPLIFE bruger denne systembrugere samt SAML tokens til at anmode SP-Link om den ønskede patientjournal.

SP-Link henter patientjournaler baseret på SAML tokens fra SPLIFE, og de leveres til de kommunale brugeres browser.

Sekvensdiagram i Figur 2 beskriver flowet gennem de forskellige systemer ved kommunale brugers klik på et deeplink.



Figur 2: Tilgang til patientjournal fra en kommunale system

## Tilgængelig miljøer

SPLIFE findes i to miljøer som kommunerne kan få adgang til, ekstern test og produktion. De to miljøer svarer til Kombit Context Handlerens ekstern test og produktion 1-1.

Tabel 1 viser de domains og porte kommunerne skal have portåbninger til hvis de ønsker at deres brugere kan tilgå patientjournaler på SP Link gennem SPLIFE.

Tabel 1: Domains og porte

Miljø	Domain	Port
Ekstern test	<a href="https://splinktest.sundhedsplatformen.dsdn.dk">https://splinktest.sundhedsplatformen.dsdn.dk</a>	443
Produktion	<a href="https://splink.sundhedsplatformen.dsdn.dk">https://splink.sundhedsplatformen.dsdn.dk</a>	443

## Sikkerhed

Alt trafik sker med HTTPS over port 443.

Adgang til SPLIFE er beskyttet med ASP.NET web forms sikkerhed. Kommunikation mellem SPLIFE og Kombit Context Handler er krypteret med SHA256 og signeret med SPLIFEs FOCES certifikat. Kommunikation mellem SPLIFE og SP Link er signeret med SPLIFEs FOCES certifikat.

Adgang til SPLIFE er begrænset til aktører indenfor Sundhedsdatanettet. Der er ingen adgang udefra.

## Krav til brugere

Brugere skal bruge en browser som opfylder krav som stilles af SP Link og Kombit Context Handler. Den eneste krav SPLIFE stiller er understøttelse af JavaScript.

For at kommunale brugere kan få adgang til SP Link gennem SPLIFE skal kommunen i det ønskede miljø have

1. delegeret en Jobfunktionsrolle som er knyttet til den korrekte Brugersystemrolle
2. den kommunale IdP registreret hos Kombit

Den brugersystemrolle som bruges til at tilgå patientjournaler på SP Link gennem SPLIFE er "Sundhedsplatformen-Læs-Journal".

I ekstern test miljø er "Sundhedsplatformen-Læs-Journal" knyttet til jobfunktionsrolle "SP Link" som kan delegeres til de kommuner som skal have adgang til at teste adgang til patientjournaler på SP Link gennem SPLIFE. For at få adgang skal der sendes en e-mail til [anne.danborg@regionh.dk](mailto:anne.danborg@regionh.dk).

Rollen er ikke tilgængelig i produktion endnu.

## Brug af SPLIFE

For at tilgå en patientjournal på SP Link gennem SPLIFE skal et såkaldt deeplink oprettes på en website ind i kommunens system. Dette link burde placeres på en website som kræver login for at sikre en gyldig login session allerede før brugeren klikker på linket.

Linket skal indeholde URL til SPLIFEs login-side (Tabel 2) samt en query string som indeholder parametre som identificer både bruger og den ønskede patient (Tabel 3). Alle parametre i tabellen er obligatoriske. Yderligere parametre bliver ignoreret. Navnet i navn-værdi par er ikke case sensitive. Værdien er case sensitive.

Tabel 2: URL til SPLIFE

Miljø	URL
Ekstern test	<a href="https://splinktest.sundhedsplatformen.dsdn.dk/splife/login.aspx">https://splinktest.sundhedsplatformen.dsdn.dk/splife/login.aspx</a>
Produktion	<a href="https://splink.sundhedsplatformen.dsdn.dk/splife/login.aspx">https://splink.sundhedsplatformen.dsdn.dk/splife/login.aspx</a>

Tabel 3: Parametre til SPLIFE

Navn	Værdi	Notat
cpr	Brugerens CPR-nummer	10 numeriske tegn uden pindestreg
id	Brugerens bruger id	Bruger id på kommunens IT-system

<b>name</b>	Brugerens fulde navn	URL encoded, f.eks. "Jens Testman" bliver til "Jens%20Testman"
<b>sorid</b>	Brugerens SOR id	SOR id på brugerens organisatoriske enhed fra SOR registret
<b>municipality</b>	Brugerens kommunekode	3 numeriske tegn, f.eks. "101" for Københavns Kommune
<b>patient</b>	CPR-nummer til patienten	10 numeriske tegn uden bindestreg

Eksempel af gyldig deeplink i ekstern test:

[https://splinktest.sundhedsplatformen.dsdn.dk/splife/login?cpr=\[cpr\]&id=\[id\]&name=\[name\]&sorid=\[sorid\]&municipality=\[municipality\]&patient=\[patient\]](https://splinktest.sundhedsplatformen.dsdn.dk/splife/login?cpr=[cpr]&id=[id]&name=[name]&sorid=[sorid]&municipality=[municipality]&patient=[patient])

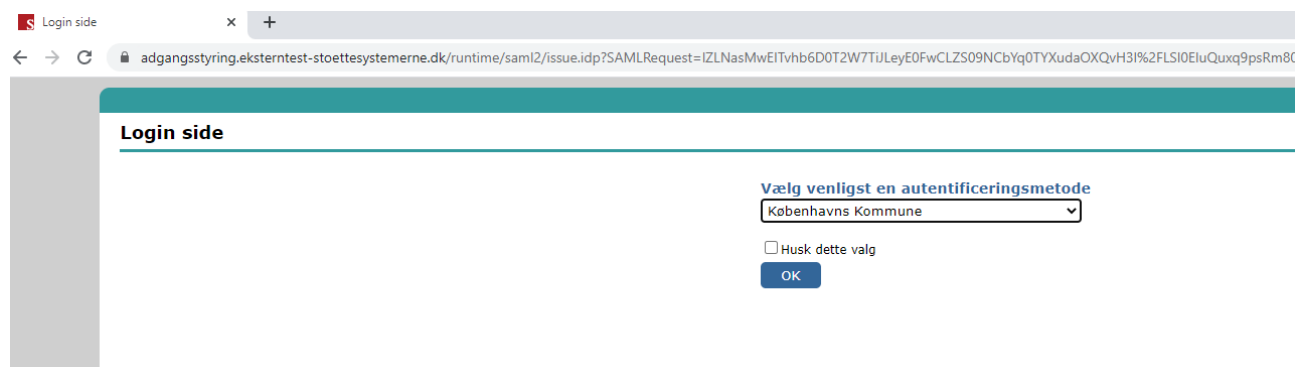
Eksempel af gyldig deeplink i produktion:

[https://splink.sundhedsplatformen.dsdn.dk/splife/login?cpr=\[cpr\]&id=\[id\]&name=\[name\]&sorid=\[sorid\]&municipality=\[municipality\]&patient=\[patient\]](https://splink.sundhedsplatformen.dsdn.dk/splife/login?cpr=[cpr]&id=[id]&name=[name]&sorid=[sorid]&municipality=[municipality]&patient=[patient])

Hvis brugeren er allerede logget ind får de adgang til patientjournal ved at klikke på deeplinket uden at de behøver at foretage sig yderligere autentificering.

I SP (systemmæssigt) bliver brugeren oprettet og aktiveret ved 1. kald. Ved efterfølgende døgn bliver brugeren inaktiveret i SP. Ved nyt opslag, bliver brugerne genaktiveret automatisk.

Skulle brugeren ikke være logget ind f.eks. fordi brugerens session er udløbet, eller fordi linket ikke var på en side som krævede login, vil brugeren omdirigeres til en "Discovery Page" hos Kombit Context Handler (Figur 3). Her vælges kommune på en dropdown hvis dette valg ikke allerede er gemt i brugerens browser. Fra Kombit Context Handler vil brugeren blive omdirigeret automatisk til den valgte kommunens login side. Efter succesfuldt login bliver brugeren omdirigeret til SP-Link og den ønskede patientjournal.



Figur 3: Valg af autentificeringsmetode på Kombit Context Handler

## Opsætning i Cura

Frederiksberg Kommune har delt dette dokument som hjælp til CURA-kommuner.

Opsætningen sker under Features (nr 15). Det er vigtigt du ikke laver dine "egne navne" under paramname.

Fx (Se sidste parameter 5), her er det vigtigt du bruger ordet patient og ikke ordet borger. Og husk ingen kan komme igennem, hvis de ikke er oprettet i "KOMBITs kontekst handler".

```

▼ 15 {5}
  name : External Links configuration
  type : externallinksconfiguration
  description : Enablement of external links
  isExternallinksEnabled :  true
▼ links [7]
  ▼ 0 {5}
    linkText : SP-link
    linkUrl1 : https://splink.sundhedsplatformen.dsdn.dk/splife/login.aspx
    reuseWindow :  true
    ► context [1]
    ▼ parameters [6]
      ▼ 0 {2}
        paramName : sorid
        value : ${orgSORID}
      ▼ 1 {2}
        paramName : municipality
        value : 147
      ▼ 2 {2}
        paramName : cpr
        value : ${userCpr}
      ▼ 3 {2}
        paramName : id
        value : ${username}
      ▼ 4 {2}
        paramName : name
        value : ${userFullName}
      ▼ 5 {2}
        paramName : patient
        value : ${citizenCpr}

```

## Logning

SPLIFE logger alle requests samt alle indsendte parametre i SPLIFE. Denne log viser alle indsendte parametre i klartekst. Loggen viser om brugeren er autentikeret og får adgang til SPLIFE.

SPLIFE logger alle tekniske fejl som sker mellem modtagelse af requests fra de kommunale sundhedssystemer og posting af SAML token til Sundhedsplatformen. SPLIFE kender ikke til fejl som muligvis sker i Sundhedsplatformen, eller om brugeren bliver nægtet adgang til patientjournal.

SP gemmer alle de informationer der er modtaget via query-string i kaldet til SPLIFE. SP Link logger yderligere visningen af patientjournalen og alle de handlinger der foretages i journalen. Denne log videregives til MinLog. På MinLog bliver CPR-numres sidste 4 tal skjult.