

GUIDE TIL ANVENDELSE AF FMK-ONLINE VIA SIKKER BROWSER OPSTART V2

Versionering

Version	Dato	Forfatter	Ændring
1.0	17-03-2015	JSO/Trifork	Første udgave
1.1	08-11-2017	JSO/Trifork	Ny organisationstype apotek, og ny parameter onBehalfOfCpr. Præciser at parametre kan sendes både som POST og query-parametre.
1.2	31-07-2019	JSO/Trifork	Ny parameter –'requestedRole' for bedre håndtering af rollevalg ifm. ny rolle behandlerfarmaceut.
1.3	16-11-2020	JSO/Trifork	Tilføj SOR som mulig organisationskode
1.4	28-11-2022	JSO/Trifork	Tilføj at Issuer-elementet skal udfyldes med korrekt STS entity-id
1.5	05-02-2025	JSO/Trifork	Tilføj anbefaling om at bruge requestedRole til at udpege rollen apoteksansat.

Indhold

Versionering	2
Indhold	3
Målgruppe	4
Baggrund	4
SIKKER BROWSEROPSTART VERSION 1 OG 2	4
Anvendelse af Sikker Browseropstart i fagsystem	4
OMVEKSLING AF SOSI IDKORT TIL SAML-ASSERTION	5
Indlejring af SAML assertion i SAML Response	5
POST af SAML Response fra webapplikation i fagsystem	6
Valg af rolle	8
Referencer	9

Målgruppe

Dette dokument retter sig imod udviklere af sundhedsfaglige it-systemer, der vil integrere FMK-online i deres løsning.

Baggrund

Der eksisterer en række centrale webservices inden for sundhedsområdet som it-fagsystemer kan integrere med, så som FMK (Fælles MedicinKort), DDV (Det Danske Vaccinationsregister), TAS (TilskudsAdministrationsService) og BEM (BEMyndigelsesservice). Det er generelt ikke nogen lille opgave at lave en sådan integration, og de forskellige services kan være mere eller mindre centrale i forhold til et fagsystems fokus. For at tilbyde en lettere integration med de bagvedliggende services, er der lavet mulighed for, at et fagsystem kan integrere med FMK-online webløsningen, sådan at den login-session og det patientvalg som brugeren har foretaget i fagsystemet kan videreføres i FMK-online. Mekanismen til at videreføre login/patientvalg fra fagsystem til FMK-online kaldes Sikker Browseropstart.

SIKKER BROWSEROPSTART VERSION 1 OG 2

FMK-online har i en årrække implementeret en ældre version af Sikker Browseropstart, kaldet "version 1". Denne løsning blev udviklet på et tidspunkt, hvor der ikke fandtes en standardiseret mekanisme, og er på nuværende tidspunkt taget ud af drift. Nærværende dokument beskriver den løsning, der kaldes "Sikker browseropstart version 2".

Anvendelse af Sikker Browseropstart i fagsystem

En forudsætning for at kunne tilgå FMK-online via Sikker Browseropstart er, at fagsystem har dannet et SOSI idkort, der repræsenterer brugerens login-session på fagsystemet. Det samme idkort bruges i de tilfælde hvor fagsystemet også laver direkte webservicekald til fx FMK. Trækning og signering af SOSI idkort er ikke beskrevet her, men er dokumenteret i (Lakeside, 2014)

Givet at fagsystemet har dannet et idkort for brugeren, er de nødvendige skridt for at tilgå FMK-online via Sikker Browseropstart i kort form:

1. Idkortet omveksles til en SAML assertion via et webservicekald til SOSI STS.
2. Den modtagne SAML assertion indlejres i et SAML Response.

3. Fagsystemet udstiller en webapplikation for brugeren, som brugerens browser dirigeres til. Denne webapplikation sender et response til brugerens browser, som indeholder en HTML FORM, som automatisk POST'es til FMK-online ved load. Denne FORM indeholder ovennævnte SAML assertion i base64 enkoded form.
4. FMK-online accepterer den POST'ede SAML assertion, og brugeren er nu logget ind.

Disse skridt er beskrevet i større detalje i det følgende. Den relevante API er generelt beskrevet i (Lakeside, 2014).

OMVEKSLING AF SOSI IDKORT TIL SAML-ASSERTION

SOSI idkortet omveksles til en SAML-assertion via et webservice-kald til STS. Se (NSI) for beskrivelse af omveksling fra SOSI idkort til SAML assertion (afsnit 7 beskriver overordnet den relevante omveksling, afsnit 8 indeholder links til eksempelkode: IDcardToOIOSAMLExample.java). Der skal ved omveksling angives et "audience". Den relevante værdi for audience er for NSI's testmiljøer en af følgende:

- "https://saml.test1.fmk.netic.dk/fmk/"
- "https://saml.test2.fmk.netic.dk/fmk/"
- "https://saml.prodtest.fmk.netic.dk/fmk/"
- "https://saml.udd.fmk.netic.dk/fmk/"

Audience for FMK-online produktion er "https://saml.fmk.staging.fmk-online.dk" (dette er den korrekte værdi for produktion, selvom værdien kunne antyde noget andet).

INDLEJRING AF SAML ASSERTION I SAML RESPONSE

Den modtagne SAML assertion skal efterfølgende indsættes i en SAML Response xml-struktur. Det opbyggede SAML Response skal have følgende form.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer>TEST1-NSP-STS<saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:EncryptedAssertion>...</saml:EncryptedAssertion>
</samlp:Response>
```

saml:Issuer skal indeholde entity-id for den STS-instans, der har foretaget den ovennævnte omveksling af idkort til SAML-assertion.

I skrivende stund accepterer FMK-online flg. STS entity-id'er i produktion:

CNSP-NSP-STs, RH-NSP-STs, RM-NSP-STs, RN-NSP-STs, RS-NSP-STs, RSJ-NSP-STs, RSP1-NSP-STs, RSP2-NSP-STs

Og flg. i de 4 NSI test-miljøer:

TEST1-NSP-STs, TEST2-NSP-STs, UDD-NSP-STs, PRODTES-NSP-STs

saml:EncryptedAssertion elementet repræsenterer svaret fra omvekslingen af idkort til SAML assertion i STS, og er her vist i forkortet form.

POST af SAML Response fra webapplikation i fagsystem

For at tilgå FMK-online via Sikker Browseropstart, skal brugerens browser POST'e en HTML FORM med det opbyggede SAML Response til FMK-online. Dette kan fx opnås ved at fagsystemet udstiller en webapplikation, der kan returnere et response med et onload script, der POST'er formen. Dette response kan opbygges således:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>SAML 2.0 POST</title>
</head>
<body onload="document.forms[0].submit()">
    <form action="http://test1.fmk.netic.dk/fmk/sboLogin" method="post">
        <input type="hidden" name="SAMLResponse" value="..." />
        <input type="hidden" name="yder" value="718122" />
        <input type="hidden" name="cpr" value="0202441041" />
    </form>
</body>
</html>
```

SAMLResponse-parameterens tilhørende value er her vist forkortet i form, men skal indeholde en base64 enkodet repræsentation af det opbyggede SAML Response.

Indholdet af action attributten afspejler hvilket FMK-online miljø, der ønskes brugt (test eller produktion). Action attributten kan starte med en af følgende url'er, hvor den første er FMK-online produktionsmiljøet og de sidste 4 er NSI's testmiljøer:

- <https://fmk-online.dk/fmk/sboLogin>
- <https://test1.fmk.netic.dk/fmk/sboLogin>

- <https://test2.fmk.netic.dk/fmk/sboLogin>
- <https://prodtest.fmk.netic.dk/fmk/sboLogin>
- <https://udd.fmk.netic.dk/fmk/sboLogin>

Parametre kan angives som POST parametre (som vist ovenfor) eller som http query parametre. Det anbefales generelt at benytte POST parametre, da man dermed undgår, at parameterværdierne fremgår af browserens url-historik.

Den fulde liste af supporterede parametre er:

- **sks**: Angiver brugerens organisation som en sks-kode.
- **yder**: Angiver brugerens organisation som et ydernummer.
- **kommune**: Angiver brugerens organisation som et kommunenummer.
- **apotek**: Angiver brugerens organisation som et ean-lokationsnummer.
- **sor**: Angiver brugerens organisation som et sor-id.
- **onBehalfOf**: Angiver hvilket autorisationsid brugeren arbejder i kraft af. Dette kan både være autorisationsid på personen, som brugeren arbejder på vegne af eller – hvis brugeren har mere end én autorisations – det valgte autorisationsid.
- **onBehalfOfCpr**: Angiver CPR-nummer for den person, brugeren arbejder på vegne af. Dette er relevant, hvis brugeren er bemyndiget af en person, der ikke har en relevant sundhedsfaglig autorisation (gælder apoteksansatte, der vil være bemyndiget af den apoteker, de er ansat hos).
- **requestedRole**: Angiver en ønsket rolle når brugeren har flere mulige roller. Se uddybning nedenfor.
- **cpr**: CPR-nummer for den valgte patient.

Ingen af disse parametre er obligatoriske. Hvis én eller flere parametre udelades, vil FMK-online i stedet prompte brugeren for evt. manglende information.

VALG AF ROLLE

Hvis en bruger kun har en mulig rolle i FMK-online, er det generelt ikke nødvendigt at gøre yderligere ifm. rollevalg, da FMK-online automatisk vil tildele brugeren den ene mulige rolle. Mange brugere vil imidlertid have flere mulige roller. Hvis den ønskede rolle ikke angives via SBO, vil FMK-online spørge brugeren, hvilket måske ikke er ønskværdigt i alle tilfælde. Typiske eksempler på brugere, der har flere mulige roller:

- Brugeren har en autorisation som læge, men også en tidligere autorisation som sygeplejerske.
- Brugeren er bemyndiget som apoteksansat, men har også en autorisation som behandlerfarmaceut.
- Brugeren er apoteker, men har også en autorisation som behandlerfarmaceut.
- Brugeren er bemyndiget som medhjælp for mere end én læge.
- Brugeren er bemyndiget som medhjælp for en eller flere læger, men har samtidig selv en autorisation som fx sygeplejerske.

Parametrene `onBehalfOf`, `onBehalfOfCpr` og `requestedRole` kan benyttes til at angive den ønskede rolle, så det kan undgås, at brugeren promptes af FMK-online. Der er generelt frit valg imellem at benytte `onBehalfOf`/`onBehalfOfCpr` eller `requestedRole` til at indikere det ønske rollevalg, dog med flg. begrænsninger:

1. Den eneste måde, at indikere, at rollen apoteker ønskes er via parameteren `requestedRole`
2. Assistent for <autoriseret sundhedsfaglig person> kan i mange tilfælde ikke vælges via `requestedRole`, fordi brugeren er bemyndiget af mere end én, og `requestedRole` dermed ikke er entydig.
3. For rollerne apoteker, apoteksansat og behandlerfarmaceut: Hvis FMK-online ikke er i stand til at verificere, at det valgte apotek er tilknyttet til den aktuelle bruger, promptes brugeren for arbejdssted og dermed også for rolle (da det foregår i den samme dialog).

`requestedRole` kan pt antage flg. værdier (parenteserne med de danske betegnelser skal ikke medtages). Ikke alle værdier giver mening ifm. SBO:

- doctor (Læge)
- dentist (Tandlæge)
- midwife (Jordemoder)
- nurse (Sygeplejerske)
- sosuassist (Social- og sundhedsassistent)
- sosuhjelp (Social- og sundhedshjælper)

- healthvisitor (Sundhedsplejerske)
- pharmacist (Farmaceut)
- pharmaconomist (Farmakonom)
- chemist (Apoteker)
- municipalemmployee (Kommunal ansat til medicinhåndtering)
- pharmacy employee (Apoteksansat)
- pharmacist with prescription rights (Behandlerfarmaceut)
- assistant for doctor (Assistent for Læge)
- assistant for dentist (Assistent for Tandlæge)
- assistant for midwife (Assistent for Jordemoder)
- assistant for nurse (Assistent for Sygeplejerske)
- assistant for sosuassist (Assistent for Social- og sundhedsassistent)
- assistant for pharmacist (Assistent for Farmaceut)
- assistant for pharmaconomist (Assistent for Farmakonom)
- assistant for sosuhelp (Assistent for Social- og sundhedshjælper)
- assistant for healthvisitor (Assistent for Sundhedsplejerske)
- assistant for chemist (Assistent for Apoteker)
- citizen (Borger)
- parentauthority (Forældermyndighed)
- guardian (Værge)
- system (System)
- supporter (Supporter)
- pharmacy system (Apotekersystem)
- Prescription Registrar (Receipt registrar)
- citizen with read right (Borger med læsefuldmagt)
- citizen with write right (Borger med handlingsfuldmagt)
- citizen with procuration (Borger med fuldmagt)
- anonymous (Anonym)
- webadmin (Web administrator)

UDPEGNING AF ROLLEN APOTEKSANSAT UDEN BRUG AF CPR

Det kan være problematisk at udpege rollen som apoteksansat via onBehalfOfCpr-parameteren, da det eksponerer apotekerens CPR-nummer i det initiale kald til FMK-online. Det anbefales derfor, at rollen som apoteksansat udpeges vha requestedRole-parameteren. **Bemærk, at for at sikre, at requestedRole**

entydigt kan udpege rollen, bør bemyndigelser som apoteksansat generelt oprettes som CVR-begrænsede bemyndigelser. CVR-begrænsningen sikrer, at kun de bemyndigelser, hvor CVR-nummeret matcher brugerens aktuelle login, vil blive taget i betragtning.

Hvis bemyndigelser oprettes uden CVR-begrænsningen, vil rollevalget via `requestedRole` i mange tilfælde ikke være entydigt, da bemyndigelser fra fx en tidligere arbejdsplads eller en tidligere apoteker på samme arbejdsplads vil kunne forstyrre.

Referencer

Lakeside. (2014). *The SOSI Library - Programmers Guide*.

NSI. (u.d.). STS - Billetomveksling. Hentet fra <https://www.nspop.dk/display/web/STS+-+Billetomveksling>