STATENS SERUM INSTITUT | NATIONAL SUNDHEDS-IT

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

STATENS SERUM INSTITUT | NATIONAL SUNDHEDS-IT

Indhold

GUIDE TIL ANVENDELSE AF FMK-ONLINE VIA SIKKER BROWSER OPSTART V2 1
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
Referencer 7

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” i det følgende. Denne løsning blev udviklet på et tidspunkt, hvor der ikke fandtes en standardiseret mekanisme. Ydermere er der tekniske begrænsninger i version 1, der betyder at visse bagvedliggende services ikke kan kaldes på vegne af brugeren. Dette betyder at tilskudsfunktionalitet og bemyndigelsesregistrering er blændet af for brugere, der tilgår FMK-online via Sikker Browseropstart version 1.

På grund af ovennævnte forhold bør nye og gamle anvendere af FMK-online via Sikker Browseropstart benytte version 2, som er beskrevet i nærværende dokument. Version 1 vil blive udfaset snarest muligt efter overgangen til 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 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: OIOSAMLToIDCardExample.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">
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:EncryptedAssertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">...</saml:EncryptedAssertion>
</samlp:Response>
```

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?yder=718122&
cpr=0202441041" method="post">
            <input type="hidden" name="SAMLResponse" value="..." />
      </form>
</body>
</html>
```

Attributten value er her vist forkortet i formen, 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) og angiver endvidere valg af organisation, autorisationsnummer (på vegne af eller egen autorisation hvis brugeren har flere autorisationer), samt patient-cpr. 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 angives med standard http request parameter syntax. 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.

- **onBehalfOf**: Angiver hvilket autorisationsid brugeren arbejder i kraft af. Dette kan både være autorisationsid på person, som brugeren arbejder på vegne af eller – hvis brugeren har mere end én autorisation – det valgte autorisationsid.
- **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.

Referencer

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

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