SUNDHEDSDATA-
STYRELSEN

Integration til SEB-IdP

i forbindelse med klargøring til MitId og Nemlog-in3

Denne vejlednings formål er at give en teknisk oversigt og vejledning for hvordan web-baserede løsninger på sundhedsområdet kan koble sig på SEB login-løsningen for borgere og medarbejdere.

Indholdsfortegnelse

1. Overblik over integrationsmuligheder

SEB Sundheds-IdP er en national login-tjeneste, der kan benyttes af web-baserede applikationer på sundhedsområdet til at autentificere brugere på højt niveau via SAML protokollerne.

Udover det, udsteder SEB digitale adgangsbilletter (tokens), der af web-baserede applikationer kan benyttes til at foretage viderekald til bagvedliggende tjenester på brugerens vegne.

Slutteligt indeholder SEB et rolle/rettighedsmodul, der kan anvendes af brugerorganisationer til at administrere egne brugeres roller/rettigheder i SEB-tilsluttede webapplikationer centralt.

SEB vil desuden kunne sættes op til at indgå i føderation med brugerorganisationers egne IdP'er og derved muliggøre fødereret brugerstyring.

2. Tilslutningsguide til SEB IdP

SEB er opdelt i en SEB IdP til borgerrettede løsninger og en SEB IdP til medarbejderrettede løsninger.

SEB testmiljøet består af nedenstående IdP'er:

- https://t-borger.dkseb.dk/runtime/ - borgerrettede løsninger
- https://t-seb.dkseb.dk/runtime/ - medarbejderrettede løsninger

SEB produktionsmiljøet består af nedenstående IdP'er:

- https://borger.dkseb.dk/runtime/ - borgerrettede løsninger
- https://seb.dkseb.dk/runtime/ - medarbejderrettede løsninger

Integration fra en webapplikation til SEB IdP'en (og derigennem med NemLog-in, samt regioners og kommuners lokale IdP'er) kan nedbrydes i følgende trin.

Integration til SEB IDP

1. Kontakt servicedesk@sundhedsdata.dk med ønske om tilslutning til SEB med info om kontaktinformation.
2. SEB Systemadministrationen kontakter Serviceejeren mhp afklaring af tilslutning og udfyldelse af "SEB Tilslutningsblanket Teknisk implementering"
3. Indgå formel tilslutningsaftale "SEB Tilslutningsaftale med Serviceejer"
4. Udveksling af SAML metadata med T-SEB IdP ud fra metadata URL, så der kan etableres en tilslutning mellem IdP'en og test-webapplikationen
5. Etablering af login-funktionalitet på test-webapplikationen, således autentificeringen foregår gennem T-SEB IdP'en
6. Etablering af logout funktionalitet på test-webapplikationen, således der logges ud af både webapplikationen og T-SEB IdP'en
7. Klarmelding af test til SEB Systemadministration.
8. Udveksling af SAML metadata med SEB IdP ud fra metadata URL, så der kan etableres en tilslutning mellem IdP'en og webapplikationen
9. Etablering af login-funktionalitet på webapplikationen, således autentificeringen foregår gennem SEB IdP'en
10. Etablering af logout funktionalitet på webapplikationen, således der logges ud af både webapplikationen og SEB IdP'en
11. Klarmelding af produktion til SEB Systemadministration.

2.1. OIOSAML bibliotekerne

Der findes to reference implementationer af OIOSAML standarden, en til Java[1] og en til .NET[2], som med fordel kan benyttes til at implementere SAML protokollerne. Begge versioner er open source samt veldokumenterede, så benyttes Java eller .NET anbefales det at benytte en af disse biblioteker. Ellers bør der benyttes en standard SAML implementation, som så konfigureres til at overholde OIOSAML profileringen[3].

2.2. Udveksling af SAML metadata

For at integrere med SEB IdP'en skal der udveksles SAML metadata med den. SAML metadata er en kontrakt, som fortæller hvem webapplikationen (i rollen som SAML serviceprovider / SP) er, hvilke certifikater der benyttes, samt hvilket grænseflader der benyttes.

Der skal konfigureres to filer med metadata, en fra IdP'en (fås fra SEB), og en fra SP'en.

IdP metadata fortæller hvilke bindings (protokoller), samt hvilke certifikater som bruges til at kontrollere signering samt til at kryptere. OIOSAML implementationen ved ud fra dette metadata hvilke certifikater som skal bruges hvor.

SAML 2.0 metadata for SEB IdP'erne kan hentes på hhv.:

[1] Se https://digitaliser.dk/resource/3920434
[2] Se https://digitaliser.dk/resource/2972745
[3] Se https://digitaliser.dk/resource/2377872

- TEST medarbejder https://t-seb.dkseb.dk/runtime/saml2/metadata.idp (SAML 2.0 metadata til medarbejderløsninger)
- TEST borger: https://t-borger.dkseb.dk/runtime/saml2/metadata.idp (SAML 2.0 metadata til borgerløsninger)

- PROD medarbejder https://seb.dkseb.dk/runtime/saml2/metadata.idp (SAML 2.0 metadata til medarbejderløsninger)
- PROD borger: https://borger.dkseb.dk/runtime/saml2/metadata.idp (SAML 2.0 metadata til borgerløsninger)

SP metadata skal konfigureres i SEB-IdP'en, og fortæller SEB-IdP'en hvilke bindings (protokoller), samt hvilke certifikater som kan bruges til at kontrollere signering samt til at kryptere. OIOSAML implementationen ved ud fra dette metadata hvilke certifikater som skal bruges hvor.

Det to OIOSAML implementationer indeholder funktionalitet til generering af SP metadata, hvilket er nærmere beskrevet i dokumentationen af OIOSAML bibliotekerne.

I OIOSAML er det kun redirect bindings som bruges.

Metadata skal genereres af SP (webapplikationen) og skal udveksles med SEB.

2.2.1. Eksempel på SP Metatdata

Eksempel på SP metadata (certifikater er forkortet af med '...'):

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="demo.serviceprovider"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   <md:SPSSODescriptor AuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="signing">
         <ds:KeyInfo>
            <ds:X509Data>
               <ds:X509Certificate>
MIIFITCCBIqgAwIBAgIEQDa1...</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://saml.serviceprovider.com:8080/saml/saml/LogoutServiceHTTPRedirect"
ResponseLocation="https://saml.serviceprovider.com:8080/saml/saml/LogoutServiceHTTPRedirectRes
ponse"/>
      <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact" Location="https://saml.serviceprovider.com:8080/saml/saml/SAMLAssertionConsumer"
index="0"/>
   </md:SPSSODescriptor>
```

2.2.2. For medarbejdervendte tilslutninger

Udover udveksling af SAML metadata skal der for medarbejdervendte løsninger tages stilling til hvorvidt følgende oplysninger skal inkluderes i SEB tokenet:

- Sundhedsfaglige autorisationer
- Oplysninger om erhvervsmæssige tilknytninger til yderorganisationer
- SEB-administrerede roller/rettigheder for webapplikationen
- SEB-administrerede nationale roller
- Bootstraptoken, der via SOSI STS kan omvekles til SOSI IdKort.

2.2.3. Koordinering af SEB-tilslutninger

Kontakt SEB metadata koordinator funktionen på Servicedesk@sundhedsdata.dk, der koordinerer indlæsning af SP-metadata samt etablering af konfiguration der er relevant for medarbejdervendte løsninger med SEB's leverandør.

2.3. Etablering af login funktionalitet i webapplikationen

Bruges OIOSAML reference-implementationerne skal der laves en loginknap, link eller lignende der rammer URL'en /saml/login/saml/* som er reference-implementationernes SAML dispatcher, som ser i IdP metadata, hvilken IdP loginside der skal rammes, og redirecter efterfølgende til denne URL. Herfra er det IdP'ens ansvar at brugeren autentificeres korrekt. Når dette er sket, returneres loginbilletten (et SAML token) fra IdP'en til SP'en, som så skal dekryptere og validere det og efterfølgende logge brugeren ind.

Bemærk, at login-flowet ikke må implementeres i en separat iFrame, da NemLog-in ikke må frames.

2.4. Etablering af logout funktionalitet i webapplikationen

Bruges reference-implementationerne skal der ligeledes laves en logout knap, link eller lignende, der rammer URL'en /saml/logout. Igen ser reference-implementationernes dispatcher i IdP metadata, hvilket logout url der skal rammes, efterfølgende redirecter IdP'en til SP'en logout-url, hvorpå sessionen nedlægges, og brugeren dermed er logget ud.

Bemærk, at logout derimod godt må foregå i en (usynlig) iFrame, men vær opmærksom på ikke at kalde logout direkte fra Javascript, idet SEB/NemLog-ins cookies da vil optræde som tredjeparts cookies, som i nogle browsere per default er slået fra og logout derfor vil fejle.

2.5. FAQ til SEB-tilslutning

Følgende er en liste af problemer der ofte forekommer ved tilslutning og hvad årsagen er:

Jeg får "Signature validation" fejl, når jeg modtager token fra SEB	Denne fejl skyldes oftest, at token signing certifikat som SEB anvender ikke trustes på din server. Problemet kan løses på to måder: 1. Sikre at der kan foretages spærrelisteopslag for token

	signing certifikat som SEB benytter. Specifikt skal der kunne foretages spærreliste opslag til OCES spærrelister i DanID testmiljø 2. De-aktivere spærrelisteopslag, ved at sætte certificatevalidation elementet i web.config til SelfIssuedCertificateSpecification (hvis OIOSAML.NET benyttes) Pkt 2 er oftest den lettest løsning, men anbefales kun til testmiljøet. I produktionsmiljøet bør der benyttes spærrelisteopslag.
Jeg får “connection not found” fejl fra SEB når jeg forsøger at logge ind.	Denne fejl forekommer, hvis der ikke er oprettet en forbindelse til jeres applikation på SEB. Tag fat i SEB Support og få dem til at hjælpe jer med at oprette en forbindelse til jeres applikation.
Skal min applikation benytte HTTPS eller er HTTP ok?	Jeres applikation skal benytte HTTPS. Føderationsprotokollerne kræver, at jeres applikation benytter HTTPS.
Skal jeg købe et certifikat til føderationen eller kan jeg lave mit eget?	Du behøver ikke købe et certifikat til føderationen. Det anbefales, at du selv generer certifikatet.

2.6. Håndtering af SAML assertion

Når brugeren er korrekt autentificeret via SEB/NemLog-in, vil en SAML assertion blive returneret til SP’en. SP’en skal dekryptere den indkommende SAML assertion og validere signatur, trust til signaturen og gyldighed i tid for assertionen – dette håndteres af standard SAML biblioteker og bør ikke kræve udvikling af applikationsspecifik kode.

Mere information vedrørende indholdet i SAML assertions og den videre adgang til de nationale sundhedsservices findes her https://www.nspop.dk/display/KLMIDNLIN3.