SUNDHEDSDATA-
STYRELSEN

Snitfladeændringer i SEB ved overgang til Mit-ID, NemLog-in3 og OCES3

V01

Overgangen til den kommende MitID, NemLog-in3 og OCES3 infrastruktur afføder ændringer til Sundhedsvæsnet Elektroniske Brugerstyring (SEB), som beskrives i dette dokument.

For en gennemgang af både nuværende og kommende anvendelsesscenarier af sundhedsvæsnets samlede nationale sikkerhedsinfrastruktur henvises til "Målarkitektur for sammenhængende brugerstyring transition 1: Overgang til MitID og NemLog-in3" (herefter blot "Målarkitekturen").

Der forudsættes at læseren har grundlæggende kendskab til nuværende SEB-komplekset, som består af både en SAML IdP (også kaldt 'SEB broker' eller 'SEB fødereret') og et bruger-rettighedskatalog (også kaldt 'SEB brugerstyring' eller 'SEB classic').

1.1. SEB SAML IdP snitflade – fagpersoner

I fagpersoners anvendelsesscenarier er der to snitflader, hvor SEB brokeren er i spil. På den ene side er der nationale webbaserede tjenester, der benytter SEB som login-punkt, og på den anden side tilbyder SEB, at lokale IdP'er kan tilsluttes i en fødereret model, som tillader decentral autentifikation og brugerrettighedsstyring.

Begge snitflader videreføres med få ændringer, som beskrives i nedenstående. De to snitflader følger OIOSAML-H profileringen, som vil blive opdateret til en ny version, som afspejler ændringerne.

SEB anvendes desuden som loginpunkt af en række SDS interne løsninger, eventuelle ændringer til denne interne brug af SEB beskrives ikke som en del af dette dokument.

1.1.1. Snitflade til tjenester som anvender SEB som login-punkt

Den tjenestevendte SAML snitflade fortsættes som integrationspunkt for nationale medarbejdervendte webbaserede applikationer, som eksempelvis Sårjournalen eller applikationer som er en del af FUT infrastrukturen.

I den nuværende SEB snitflade inkluderes et SOSI idkort for brugeren i det token SEB udsteder, som den tilgåede webapplikation kan anvende til at tilgå DGWS/SOSI-baserede service på brugerens vegne.

Indlejring af SOSI-idkort udgår og erstattes med inklusion af et SAML-baseret bootstraptoken, som aftageren i stedet kan veksle til et SOSI-idkort via SOSI-STS[1]. Derved bliver der mulighed for fastsættelse af den rette brugerkontekst i SOSI-idkortet (valgt sundhedsfaglig autorisation eller national rolle), hvilket ikke kan lade sig gøre med nuværende SEB, som eksempelvis ikke kan håndtere brugere med flere sundhedsfaglige autorisationer.

I nedenstående afsnit 1.4.1 er der vist et eksempel på en SEB udstedt OIOSAML-H assertion med et indlejret bootstrap token.

1.1.2. Snitflade til (lokale) IdP'er som føderer med SEB

Nuværende snitflade til integration af lokale IdP'er i et fødereret setup (som pt. alene anvendes af FUT infrastrukturen) videreføres – men i to varianter.

Såfremt den lokale IdP er NSIS compliant kan denne integreres med SEB ved at følge 'OIOSAML Local IdP Profile'[2], dvs. med samme profil som benyttes i en NemLog-in3 integration, hvor relevante rettigheder/privilegier som hidtil kan udtrykkes i en OIOBPP struktur.

I det omfang lokale IdP'er endnu ikke er NSIS-parate og der eksempelvis anvendes MOCES3-certifikater som overgangsløsning i organisationen, kan der fortsat fødereres med SEB efter den nuværende OIOSAML-H baserede model. Nuværende 'step-up' funktionalitet i SEB, hvor brugerorganisationer, der ikke selv kan autentificere brugere på tilstrækkelig højt niveau (med medarbejdersignatur), udgår, idet der fremover i NemLog-in3 ikke bliver mulighed for at anvende medarbejdercertifikater til autentifikation. Det bliver derfor i denne føderede anvendelse et krav, at brugeren autentificeres lokalt i brugerorganisation, og der fra den lokale IdP medsendes et gyldigt SOSI idkort som autentifikationsbevis (efter samme mekanisme som hidtil). Hvor det med andre ord hidtil har været frivilligt at medsende et SOSI-idkort (for at videreføre en eksisterende 'session' i SOSI-føderationen og undgå re-autentifikation i NemLog-in) bliver dette nu påkrævet.

I nedenstående afsnit 1.4.2 er der vist et eksempel på en lokalt udstedt SAML assertion med et indlejret SOSI-idkort.

[1] Se BST2SOSI snitfladebeskrivelsen i 'Snitfladeændringer i NSP komponenter ved overgang til MitID NemLog-in3 og OCES3 v01'
[2] Se https://digst.dk/it-loesninger/nemlog-in/det-kommende-nemlog-in/vejledninger-og-standarder/oiosaml-302/ og https://digst.dk/media/21891/oiosaml-local-idp-profile-102.pdf

1.2. SEB SAML IdP snitflade – borgervendte anvendelser

<Udestår – kommer i senere udgaver af dette dokument>

1.3. SEB brugerstyring

<Udestår – kommer i senere udgaver af dette dokument>

1.4. Eksempler

Eksemplerne i dette afsnit skal betragtes som foreløbige og ikke normative.

1.4.1. SEB-udstedt OIOSAML-H assertion for en fagperson

```
<Assertion ID="ide4e3e74b106e4a4dac91df120492a3c4" IssueInstant="2020-12-15T10:53:30.562Z"
Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
   <Issuer>https://t-seblogin.nsi.dk/runtime/</Issuer>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
         <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
         <Reference URI="#ide4e3e74b106e4a4dac91df120492a3c4">
            <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
               <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <DigestValue>KiNo...hN2ng=</DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>Kxkc...2Zg=</SignatureValue>
      <KeyInfo>
         <X509Data>
            <X509Certificate>MIIF...z9w==</X509Certificate>
         </X509Data>
      </KeyInfo>
   </Signature>
   <Subject>
      <!-- En identifikation af brugeren - indholdsformat er uspecificeret -->
      <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">Lakeside Test
Læge</NameID>
      <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
         <SubjectConfirmationData InResponseTo="id2d49ff942d9d494b945336435a3e07a4"
NotOnOrAfter="2020-12-15T10:58:30.562Z" Recipient="https://lægesystem-xyz/login.ashx" />
      </SubjectConfirmation>
   </Subject>
   <Conditions NotBefore="2020-12-15T10:53:30.562Z" NotOnOrAfter="2020-12-15T11:53:30.562Z">
      <!-- Identifikation af tjenesten der modtager assertionen -->
      <AudienceRestriction>
         <Audience>https://lægesystem-xyz</Audience>
      </AudienceRestriction>
   </Conditions>
   <AuthnStatement AuthnInstant="2020-12-15T10:53:30.562Z" SessionIndex="620811646">
      <AuthnContext>

<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified</AuthnContextClassRe
```

```
f>
      </AuthnContext>
   </AuthnStatement>
   <AttributeStatement>
      <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>DK-SAML-2.0</AttributeValue>
      </Attribute>
      <!-- 'organizationName' attributten -->
      <Attribute Name="urn:oid:2.5.4.10" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
         <AttributeValue>LAKESIDE A/S</AttributeValue>
      </Attribute>
      <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>25450442</AttributeValue>
      </Attribute>
      <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>3</AttributeValue>
      </Attribute>
      <!-- 'commonName' attributten (brugerens fulde navn) -->
      <Attribute Name="urn:oid:2.5.4.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
         <AttributeValue>Lakeside Test Læge</AttributeValue>
      </Attribute>
      <Attribute Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>0205756078</AttributeValue>
      </Attribute>
      <!-- En angivelse af hvorvidt brugeren har en sundhedsfaglig autorisation -->
      <Attribute Name="dk:healthcare:saml:attribute:HasUserAuthorization"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>true</AttributeValue>
      </Attribute>
      <!-- Brugerens sundhedsfaglige autorisationer i Base64-encoded form -->
      <Attribute Name="dk:healthcare:saml:attribute:UserAuthorizations"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>PD94...dD4=</AttributeValue>
         <!-- Attributværdi i Base64-decoded form:

         <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
         <uap:UserAuthorizationList xmlns:uap="urn:dk:healthcare:saml:user_authorization_profile:1.0">
            <uap:UserAuthorization>
               <uap:AuthorizationCode>LKS01</uap:AuthorizationCode>
               <uap:EducationCode>7170</uap:EducationCode>
               <uap:EducationType>Læge</uap:EducationType>
            </uap:UserAuthorization>
         </uap:UserAuthorizationList>

         -->
      </Attribute>
      <!-- En (optionel) angivelse af for modtageren relevante roller/rettigheder  (fx medlemskab af et
'CareTeam' i FUT) - udtrykt som OIOBPP struktur i Base64 encoded form -->
      <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>3EZi ...</AttributeValue>
      </Attribute>
      <!-- Et SAML bootstrap token i Base64-encoded form som kan veksles til et SOSI idkort ved SOSI-
STS (indhold af attributter er alene en kontrakt mellem SEB og SOSI-STS, levetid at tokenet vil dog altid
kunne aflæses) -->
      <Attribute Name="urn:liberty:disco:2006-08:DiscoveryEPR"
```

```
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <AttributeValue>bHR...ob3J</AttributeValue>
        <!-- Bootstrap-tokenet i Base64-decoded form:

        <Assertion ID="4a4dac91dfide4e3e74b106e120492a3c4" IssueInstant="2020-12-
15T10:53:30.562Z" Version="2.0"
                xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
            <Issuer>https://t-seblogin.nsi.dk/runtime/</Issuer>
            <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                ...
            </Signature>
            <Subject>
                ...
            </Subject>
            <Conditions NotBefore="2020-12-15T10:53:30.562Z" NotOnOrAfter="2020-12-
15T11:53:30.562Z">
                ...
            </Conditions>
            <AttributeStatement>
                ...
            </AttributeStatement>
        </Assertion>

        -->
    </Attribute>
  </AttributeStatement>
</Assertion>
```

1.4.2. OIOSAML-H assertion udstedt af lokal IdP til SEB

```
<Assertion ID="ide4e3e74b106e4a4dac91df120492a3c4" IssueInstant="2020-12-15T10:53:30.562Z"
Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <Issuer>https://idp.korsbaek-kommune.dk</Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <Reference URI="#ide4e3e74b106e4a4dac91df120492a3c4">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue>KiNolUfIc631xclZ9zT6ptsZ25JXU7YI4sfKrDhN2ng=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>5VS…Xsg=</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>MII...9w==</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
  <Subject>
    <!-- En identifikation af brugeren - indholdsformat er uspecificeret -->
    <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">Mads
Skjern</NameID>
    <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <SubjectConfirmationData InResponseTo="id2d49ff942d9d494b945336435a3e07a4"
NotOnOrAfter="2020-12-15T10:58:30.562Z" Recipient="https://t-seblogin.nsi.dk/runtime/login.ashx"
```

```
/>
      </SubjectConfirmation>
   </Subject>
   <Conditions NotBefore="2020-12-15T10:53:30.562Z" NotOnOrAfter="2020-12-15T11:53:30.562Z">
      <!-- Identifikation af tjenesten der modtager assertionen (her SEB) -->
      <AudienceRestriction>
         <Audience>https://t-seblogin.nsi.dk/runtime/</Audience>
      </AudienceRestriction>
   </Conditions>
   <AuthnStatement AuthnInstant="2020-12-15T10:53:30.562Z" SessionIndex="620811646">
      <AuthnContext>

<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified</AuthnContextClassRe
f>
      </AuthnContext>
   </AuthnStatement>
   <AttributeStatement>
      <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>DK-SAML-2.0</AttributeValue>
      </Attribute>
      <!-- 'organizationName' attributten -->
      <Attribute Name="urn:oid:2.5.4.10" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
         <AttributeValue>Korsbæk Kommune</AttributeValue>
      </Attribute>
      <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>20301823</AttributeValue>
      </Attribute>
      <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>3</AttributeValue>
      </Attribute>
      <!-- 'commonName' attributten (brugerens fulde navn) -->
      <Attribute Name="urn:oid:2.5.4.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
         <AttributeValue>Mads Skjern</AttributeValue>
      </Attribute>
      <Attribute Name="dk:gov:saml:attribute:CprNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>0205756078</AttributeValue>
      </Attribute>
      <!-- En (optionel) angivelse af for modtageren relevante roller/rettigheder  (fx medlemskab af et
'CareTeam' i FUT) - udtrykt som OIOBPP struktur i Base64 encoded form -->
      <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>3EZi ...</AttributeValue>
      </Attribute>
      <!-- En til SEB krypteret OIOSAML assertion med et indlejret SOSI idkort som autentifikationsbevis --
>
      <Attribute Name="dk:healthcare:saml:attribute:EncryptedOIOSamlAssertion"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
         <AttributeValue>Xs34 ...</AttributeValue>
      </Attribute>
   </AttributeStatement>
</Assertion>
```