SUNDHEDSDATA-
STYRELSEN

Snitfladeændringer i NSP-komponenter ved overgang til MitID, NemLog-in3 og OCES3

V021

Overgangen til den kommende MitID, NemLog-in3 og OCES3 infrastruktur afføder en række ændringer til NSP-sikkerhedskomponenterne, 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 kendskab til nuværende NSP- og SOSI-infrastruktur.

1.1. NSP-snitflader – fagpersoner og systemer

For fagpersoners og systemers tilgang via identitetsbaserede service-integrationer fastholdes DenGodeWebService (DGWS) version 1.0.1 som webservice-profil og dermed SOSI idkortet som adgangsbillet.

1.1.1. SOSI-STS

Som beskrevet i Målarkitekturen udbygges SOSI-STS med håndtag til at kunne understøtte OCES3-signerede idkort-requests, samt at kunne udstede SOSI idkort igennem en veksling af omvekslings-/bootstrap-tokens, som er udstedt af en lokal IdP eller den nationale Sundheds-IdP (SEB).

Konkret er det følgende STS-snitfladeændringer:

1.1.1.1. Minimale ændringer: Autentifikationssnitflade (SecurityTokenService/New-SecurityTokenService)

De nuværende STS-autentifikationssnitflader, der udsteder SOSI idkort på baggrund af henholdsvis medarbejder-signerede idkort-requests (MOCES-signeret) eller system-signerede idkort-requests (FOCES/VOCES-signerede) videreføres i deres nuværende form og udbygges til at understøtte OCES3-signerede idkort-requests.

Den nuværende NewSecurityTokenService snitflade blev introduceret i forbindelse med indføring af sikkerbrowser-opstarts konceptet og har en særlig feature, hvor indkommende Subject NameID feltet for user-idkort erstattes med oplysninger om brugerens MOCES-certifikat, der ligger til grunde for autentifikationen. Disse indlejrede certifikatoplysninger anvendes af STS'en under eventuelle efterfølgende omvekslinger af idkortet til et OIOSAML sikkerbrowser-opstarts token (for at kunne være compliant med OIOSAML2s OCES-profil). Se også afsnittet 'Subject NameID elementet i SOSI-idkort~~Subject NameID elementet i SOSI-idkort~~' for et konkret eksempel.

Med overgangen til ny MitID/NemLog-in3/OCES3 infrastruktur er bruger-autentifikation ikke nødvendigvis OCES-baseret, og STS'en kommer til at udstede SOSI-idkort, der ikke tager udgangspunkt i en OCES-autentifikation (se nedenstående 'Ny snitflade: Billetomveksling for bootstraptokens (BST2SOSI)').

Den nuværende feature, hvor Subject NameID ved kald til NewSecurityTokenService erstattes med certifikatoplysninger, fjernes i STS, så det indgående NameID bibeholdes i idkort som STS'en udsteder – dvs. NewSecurityTokenService kommer til at håndtere idkort udstedelsen præcis som (den oprindelige) SecurityTokenService.

Der vurderes umiddelbart, at denne ændringer ikke får den store betydning for parterne, idet der så vidt vides, ikke er andre komponenter end STS'en selv, der har gjort brug af denne særlige feature.

1.1.1.2. Ny snitflade: Billetomveksling for bootstraptokens (BST2SOSI)

For at understøtte de i Målarkitekturen beskrevne anvendelsesscenarier 'Føderationsscenariet: Ansattes adgang via rig klient og egne identitetsmidler' og 'MitID-scenariet: Ansattes adgang via ri klient og MitID Erhverv' indføres en ny snitflade på SOSI-STS, der kan udstede SOSI-idkort på baggrund af et IdP-udstedt omvekslings-/bootstraptoken.

Input til den nye BST2SOSI snitflade er et bootstraptoken fra en trusted og NSIS-compliant IdP og en række claims/parametre, der er nødvendige til at kunne danne et SOSI idkort med den rette kontekst.

Konkret skal en IdP være NSIS-registreret og kunne danne bootstraptokens med afsæt i det nye OIOSAML3 standard og med følgende egenskaber.

- "Subject NameID" skal indeholde en persistent og i den pågældende organisation unik ID for brugeren (fx et AD-brugernavn eller erhvervspersonens global unikke ID fra den kommende fællesoffentlige erhvervsadministration (EIA)).
- Sikringsniveau/AssuranceLevel skal angives som NSIS-niveau
- Erhvervspersonens global unikke ID fra den kommende fællesoffentlige erhvervsadministration (EIA) skal angives

- Organisationens CVR-nummer og organisations-navn skal fremgå af tokenet
- Tokenet skal indeholde en angivelse af den tiltænkte audience (SOSI-STS)
- Tokenet kan indeholdende en liste over brugerens lokalt administrerede 'nationale roller' (til brugerstyring af brugere uden sundhedsfaglige autorisation)
- Som fremtidssikring bør tokenet om muligt udformes som 'holder-of-key' token (dvs. det bindes kryptografisk til det klientsystem der varetager omvekslingen) og ikke som 'bearer' token. (Holder-of-key relationen vil ikke blive enforcet i BST2SOSI snitfladen, men forventes at komme i spil når DGWS i fremtiden erstattes af IDWS XUA sikkerhedsprofilen.)

(Kravene bliver formaliseret i en egentlig profil af den fællesoffentlige OIO Bootstraptoken profil).

I afsnittet 'Eksempel bootstraptokenBootstraptoken' er der angivet et eksempel på hvordan et IdP-udstedt bootstraptoken kunne se ud.

Til udstedelse af et SOSI-idkort kræves der, at der medsendes yderlige oplysninger som parametre i BST2SOSI-kaldet (kaldt 'claims' i den anvendte WS-Trust protokol):

- En angivelse af det kaldende it-system (en påkrævet attribut i DGWS/SOSI-idkortet)
- En (frivillig) angivelse af fagpersonens sundhedsfaglig autorisation (for at udpege den relevante, hvis personen har flere)
- En (frivillig) angivelse af fagpersonens "rolle" som skal anvendes i SOSI idkort. På lige fod som ved nuværende SOSI idkort-udstedelse kan denne rolle sættes til:
    - En uddannelseskode (fx 7170 for 'læge') til udpegning af en fagpersonens tilhørende sundhedsfaglig autorisation (hvis personen har flere)
    - En 'national rolle' som fagpersonen ønsker at anvende. (Nationale roller administreres enten centralt i SEB brugerstyring eller styres gennem trust-aftaler. Når angivelse af national rolle foregår på baggrund af en trust-aftale, skal brugerens ønskede nationale rolle fremgå af listen af mulige nationale roller i det medsendte lokalt IdP-signerede bootstraptoken.)
    - En angivelse af at ingen autorisation ønskes[1], eksempelvis i situationer hvor fagpersonen arbejder under delegering og derfor ikke ønsker at anvende en eventuel sundhedsfaglig autorisation eller i situationer hvor fagpersonen har en centralt registreret national rolle i SEB, men hvor den præcise navngivning af rollen ikke er registreret i fagsystemet.
    - ~~-~~
- En (frivillige) angivelse af et ID for fagpersonen, der ønskes som 'Subject NameID' i SOSI-idkortet (kan være relevant når SOSI-Gateway anvendes, se diskussion under 'Ny snitflade: Opret idkort i SOSI-GW ud fra bootstraptoken (createIdCardFromBST)').

[1] Angives som "urn:dk:healthcare:no-role"

SOSI-STS udsteder SOSI-idkort på baggrund af det indkommende bootstraptoken og de medsendt claims. Som 'Subject NameID' i SOSI-idkortet videreføres 'Subject NameID' fra det indkommende bootstraptoken, medmindre dette overstyres via angivelse af ID som separat claim (Der bemærkes at STS ikke vil forsøge at fortolke indholdet af NameID og 'NameID format' sættes derfor i SOSI-idkortet til 'medcom:other' jf. DGWS-standarden).

I det omfang, at STS'en ud fra inputtet ikke entydig kan fastlægge brugerens sundhedsfaglig autorisation eller tildelt 'national rolle', returneres som på autentifikationssnitfladen et passende fejlsvar. Eksempelvis vil der for en bruger med to sundhedsfaglige autorisationer returneres et fejlsvar indeholdende brugerens to mulige autorisationer. Herefter kan klientapplikationen bede brugeren om at vælge den aktuelle autorisation og gentag STS-kaldet med en angivelse af den valgte autorisation i et claim.

I afsnittene 'Eksempel BST2SOSI STS-request~~Eksempel BST2SOSI STS-request~~' og 'Eksempel BST2SOSI STS-response~~Eksempel BST2SOSI STS-response~~' er der angivet eksempler på et BST2SOSI kald og tilhørende STS-svar.

1.1.1.3. Minimale ændringer: Sikker-browseropstart billetomveksling (SOSI2OIOSAML)

Som beskrevet i ovenstående er bruger-autentifikation i den kommende infrastruktur ikke nødvendigvis OCES-baseret og SOSI-idkort kan dermed ikke længere beriges med certifikatoplysninger.

SOSI2OIOSAML snitfladen udvides derfor til også at kunne omveksle SOSI-idkort, der ikke indeholder certifikatoplysninger (se 'Subject NameID elementet i SOSI-idkort~~Subject NameID elementet i SOSI-idkort~~' for nuværende indhold med certifikatoplysninger).

I de udstedte OIOSAML tokens, der krypteres til den webapplikation som ønskes tilgået via sikker-browseropstart, indsættes da dummy-/null-værdier for de i nuværende OIOSAML2 OCES-profilen påkrævede attributter, der relaterer sig til MOCES-certifikater.

I og med OIOSAML tokenet er krypteret til webapplikationen der tilgås og dermed ikke kan læses af andre parter, har ændringen kun betydning for (den lille håndfuld af) webapplikationer, som understøtter sikker-browseropstart.

1.1.1.4. Udgår: OIOSAML/NemLog-in billetomveksling (OIOSAML2SOSI)

Nuværende OIOSAML2SOSI snitflade anvendes af webbaserede løsninger, der benytter NemLog-in til autentifikation, og som skal anvende et SOSI-idkort for at tilgå nationale DGWS-tjenester på vegne af brugeren. OIOSAML2SOSI snitfladen stammer fra tiden før parternes brokere kunne føderere med hinanden og før koncepterne omkring omvekslings-/bootstrap-tokens blev realiseret.

Snitfladen beror på en konceptuel lidt forkert tilgang, hvor omvekslingen baseres på et token (fra NemLog-in), der egentlig har et andet formål (nemlig at give brugeren adgang til en webapplikation). Snitfladen udfases med overgangen til den nye infrastruktur og funktionaliteten til at kunne danne bro mellem en web-baseret autentifikation (via den nationale Sundheds IdP, som proxy for NemLog-in, eller lokale IdP'er[2]) varetages af 'Ny snitflade: Billetomveksling for bootstraptokens (BST2SOSI)'.

1.1.2. SOSI-Gateway

SOSI-Gateway komponenten videreføres med overgangen til den nye infrastruktur, hvor den nuværende snitflade til oprettelse af et bruger-idkort i SOSI-Gateway på baggrund af et MOCES-signeret idkort request udvides til også at kunne understøttes requests signeret med det nye MOCES3.

For at understøtte parter, der etablerer egne IdP'er og som anvender SOSI-Gateway funktionalitet, udbygges SOSI-Gateway med en ny snitflade, der kan danne SOSI-idkort på baggrund at omvekslings-/bootstraptoken fra en lokal IdP.

Den nuværende anvendelses-/proxy-snitflade, der udskifter idkortet i et indkommende DGWS kald med det tilsvarende signerede idkort fra SOSI-Gateway cachen, forbliver uændret.

1.1.2.1. Ny snitflade: Opret idkort i SOSI-GW ud fra bootstraptoken (createIdCardFromBST)

Den nye 'createIdCardFromBST' snitflade på SOSI-GW udformes med præcis det samme WS-Trust baserede interface som STS'ens nye 'BST2SOSI' snitflade, se ovenstående 'Ny snitflade: Billetomveksling for bootstraptokens (BST2SOSI)'.

Input til snitfladen er således et lokal-IdP-udstedt bootstraptoken og supplerende claims. Outputtet fra den nye SOSI-Gateway snitflade er det udstedte SOSI-idkort i ikke-signeret tilstand (SOSI-Gateway fjerner signaturen). Herved fastholdes konceptet med SOSI-Gateway som en sikkerhedsgateway, der ikke udleverer signerede idkort til klienter, men hvor der gives adgang til inspektion af attributterne i det udstedte idkort.

Eventuelle fejlsvar fra STS føres tilbage til det kaldende system i uændret form.

SOSI-Gateway anvender indholdet af 'Subject NameID' fra idkortet som nøgle til indeksering af SOSI-idkort i dens cache. I praksis betyder det, at oprettelses- og anvendelses-kaldene til SOSI-Gateway skal kunne medsende samme 'Subject NameID'. I nogle brugsscenarier håndteres op-

[2] Se Målarkitekturen for en gennemgang af de fremtidige anvendelsesscenarier

rettelse og anvendelse af SOSI idkort i adskilte lokale applikationer. Eksempelvis en særskilt 'login-applikation', hvis ansvar er at oprette idkort i SOSI-Gateway, hvorimod den efterfølgende anvendelse af idkortet sker i fagsystemer kald til nationale services. Den nye 'createIdCardFromBST' snitflade på SOSI-Gateway (og STS'ens nye 'BST2SOSI' snitflade som SOSI-Gateway kalder) kan via et claim overstyre, at NameID fra bootstraptokenet anvendes som nøgle til idkortet i SOSI-Gateway. Herved fås fuld fleksibilitet i forhold til afstemning af ID'er mellem oprettelse af idkort og efterfølgende anvendelse.

Der bemærkes at 'createIdCardFromBST' snitfladen realiseres som en ren proxy snitflade i forhold til STS'ens BST2SOSI snitflade og at indkommende kald videreføres i uforandret form, som dermed også kan udformes med holder-of-key beskeds-signering. Kun ved håndtering af retursvaret modificeres kaldet igennem SOSI-Gateway, da signaturen fjernes på såvel svarbeskeden som på idkortet.

1.1.3. Afkoblingskomponent/DCC

Der er ingen ændringer i forhold til afkoblingskomponenten (DCC), som de fleste DGWS tjenester på NSP tilgås igennem.

1.2. NSP-snitflader – borgervendte anvendelser

<Udestår – kommer i senere udgaver af dette dokument>

1.3. Eksempler

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

1.3.1. Subject NameID elementet i SOSI-idkort

Nuværende NameID format som SOSI-STS generer ved medarbejder-idkort-requests til NewSecurityTokenService, hvor NameID formatet i idkort-requestet erstattes med oplysninger fra brugerens certifikat:

```
<saml:Assertion IssueInstant="2020-10-26T15:29:35Z" Version="2.0" id="IDCard">
  <saml:Issuer>TEST2-NSP-STS</saml:Issuer>
  <saml:Subject>
    <saml:NameID Format="medcom:other">SubjectDN={SERIALNUMBER=CVR:30808460-
RID:42634739 + CN=TU GENEREL MOCES M CPR gyldig, O=NETS DANID A/S // CVR:30808460,
C=DK},IssuerDN={CN=TRUST2408 Systemtest XXII CA, O=TRUST2408,
C=DK},CertSerial={1538078558}</saml:NameID>
    <saml:SubjectConfirmation>
      <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key</saml:ConfirmationMethod>
      <saml:SubjectConfirmationData>
        <ds:KeyInfo>
          <ds:KeyName>OCESSignature</ds:KeyName>
        </ds:KeyInfo>
```

```
    </saml:SubjectConfirmationData>
  </saml:SubjectConfirmation>
</saml:Subject>
```

Kommende NameID format som SOSI-STS generer ved medarbejder-idkort-requests til NewSecurityTokenService, hvor NameID formatet fra idkort-requestet videreføres (her med CPR-nummer formatet som eksempel):

```
<saml:Assertion IssueInstant="2020-10-26T15:29:35Z" Version="2.0" id="IDCard">
   <saml:Issuer>TEST2-NSP-STS</saml:Issuer>
   <saml:Subject>
      <saml:NameID Format="medcom:cprnumber">1802602810</saml:NameID>
      <saml:SubjectConfirmation>
         <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key</saml:ConfirmationMethod>
         <saml:SubjectConfirmationData>
            <ds:KeyInfo>
               <ds:KeyName>OCESSignature</ds:KeyName>
            </ds:KeyInfo>
         </saml:SubjectConfirmationData>
      </saml:SubjectConfirmation>
   </saml:Subject>
```

1.3.2. BST2SOSI billetomveksling

1.3.2.1. Eksempel bootstraptoken

Nedenfor vises et eksempel på et bootstraptoken udstedt af en fiktiv kommunes IdP. De væsentligste attributter i tokenet er fremhævet med gult, og tokenet er udformet som et holder-of-key token.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_f3070cce-b0ce-4025-b374-
ada158cb137c" IssueInstant="2020-11-13T10:22:50.027Z" Version="2.0">
   <!-- Udstederen af bootstraptokenet (her Korsbæk Kommunes IdP) -->
   <Issuer>https://idp.korsbaek-kommune.dk</Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
         <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
         <ds:Reference URI="#_f3070cce-b0ce-4025-b374-ada158cb137c">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<ds:DigestValue>mLOzno5qLFEcRB7wZ803T+63ZuUdWFETQm1DH0uLgxE=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>cam ... 6d2DQ==</ds:SignatureValue>
      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
         <X509Data>
            <!-- Certifikat som har signeret bootstraptokenet (her Korsbæk Kommunes IdP) -->
            <X509Certificate>MII ... xyg==</X509Certificate>
```

```
            </X509Data>
        </KeyInfo>
    </ds:Signature>
    <Subject>
        <!-- NameID indeholder en i organisationen unik ID for erhvervspersonen - kunne også sættes til
erhvervspersonens global unikke ID,
        som tildelt i den fællesoffentlige erhvervsadministration -->
        <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">KorsbaekKommune\MSK</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
            <SubjectConfirmationData xmlns:a="http://www.w3.org/2001/XMLSchema-instance"
a:type="KeyInfoConfirmationDataType">
                <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                    <X509Data>
                        <!-- Holder-of-key certifikatet - dvs. certifikat for det system/SOSI-STS-klient som kan
veksle bootstraptokenet til et SOSI-idkort-->
                        <X509Certificate>MII ... xjQs</X509Certificate>
                    </X509Data>
                </KeyInfo>
            </SubjectConfirmationData>
        </SubjectConfirmation>
    </Subject>
    <Conditions NotOnOrAfter="2020-11-13T12:22:50.027Z">
        <!-- Aftageren som må omveksle dette bootstraptoken (her SOSI-STS'en)  -->
        <AudienceRestriction>
            <Audience>https://sts.sosi.dk/</Audience>
        </AudienceRestriction>
    </Conditions>
    <AttributeStatement>
        <!-- Angivelse af profil og version (konstanten 'OIO-SAML-3.0') -->
        <Attribute Name="https://data.gov.dk/model/core/specVersion"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>OIO-SAML-3.0</AttributeValue>
        </Attribute>
        <!-- Sikringsniveau udtrykt efter NSIS -->
        <Attribute Name="https://data.gov.dk/concept/core/nsis/loa"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>Substantial</AttributeValue>
        </Attribute>
        <!-- Ervhvervspersonens global unikke ID, som tildelt i den fællesoffentlige erhvervsadministration -->
        <Attribute Name="https://data.gov.dk/model/core/eid/professional/uuid/persistent"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>urn:uuid:323e4567-e89b-12d3-a456-426655440000</AttributeValue>
        </Attribute>
        <!-- Organisationens CVR nummer (her Korsbæk Kommunes) -->
        <Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>20301823</AttributeValue>
        </Attribute>
        <!-- Organisationens navn (her Korsbæk Kommune) -->
        <Attribute Name="https://data.gov.dk/model/core/eid/professional/orgName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>Korsbæk Kommune</AttributeValue>
        </Attribute>
        <!-- En (frivillig) angivelse af brugerens centralt trustede og lokalt administrerede 'nationale roller'
formatteret som OIOBPP 1.2 XML struktur og indlejret i Base64 encoded form
        <Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>Bx23z ....</AttributeValue>
        </Attribute>
      Eksempel (i Base64 decoded form) for en bruger med tildelt 'national rolle' 'Plejehjemsassistent' i
Korsbæk Kommune:
```

```
    <bpp:PrivilegeList
     xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:20301823">
        <Privilege>urn:dk:healthcare:national-federation-role:code:41003:value:PlejeAssR3</Privilege>
      </PrivilegeGroup>
    </bpp:PrivilegeList>

  -->

  </AttributeStatement>
</Assertion>
```

1.3.2.2. Eksempel BST2SOSI STS-request

I nedenstående eksempel på et BST2SOSI request fra en fiktiv kommune er de væsentligste elementer fremhævet med gult. Eksemplet er udformet som kald med holder-of-key token. Det modsvarede 'createIdCardFromBST' kald til SOSI-GW vil have tilsvarende indhold.

```
<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wst="http://docs.oasis-
open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-open.org/ws-sx/ws-trust/200802"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
   <soapenv:Header>
      <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
      <wsa:MessageID wsu:Id="messageID">urn:uuid:bfe03422-990c-49ec-9a31-
07eeb82ffed3</wsa:MessageID>
      <wsse:Security mustUnderstand="1" wsu:Id="security">
         <wsu:Timestamp wsu:Id="ts">
            <wsu:Created>2020-11-12T08:09:53Z</wsu:Created>
         </wsu:Timestamp>
         <ds:Signature>
            <ds:SignedInfo>
               <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
               <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <ds:Reference URI="#messageID">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>3/bX3JnTKLfa2WHUcLHFaHbq0/k=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference URI="#action">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>3cXAhlhZH22NiSh7AttxKxBap7Q=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference URI="#ts">
                  <ds:Transforms>
```

```
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>CF/Pjtr//fCqWISF0PS7DeEjBgI=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#body">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>u2b1ztME9hJij5RJneSCwqahRM4=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>if ... Q==</ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <!-- Certifikat som har signeret beskeden (body og relevante headere)- skal matche Holder-
of-Key certifikatet i bootstraptokenet -->
              <ds:X509Certificate>MII ... xyg==</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
      </wsse:Security>
    </soapenv:Header>
    <soapenv:Body wsu:Id="body">
      <wst:RequestSecurityToken Context="urn:uuid:b216a8d9-0cab-40f7-8f60-8fa854c284a7">
        <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
        <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
        <wst14:ActAs>
          <!-- Bootstraptoken -->
          <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" ID="_f3070cce-b0ce-4025-
b374-ada158cb137c" IssueInstant="2020-11-12T07:22:50.027Z" Version="2.0">
            <!-- Udstederen af bootstraptokenet (her Korsbæk Kommunes IdP) -->
            <Issuer>https://idp.korsbaek-kommune.dk</Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
                <ds:Reference URI="#_f3070cce-b0ce-4025-b374-ada158cb137c">
                  <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />

<ds:DigestValue>mLOzno5qLFEcRB7wZ803T+63ZuUdWFETQm1DH0uLgxE=</ds:DigestValue>
                </ds:Reference>
              </ds:SignedInfo>
              <ds:SignatureValue>Zca ... DQ==</ds:SignatureValue>
              <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data>
                  <!-- Certifikat som har signeret bootstraptokenet (her Korsbæk Kommunes IdP) -->
                  <X509Certificate>MII ... xyg==</X509Certificate>
                </X509Data>
              </KeyInfo>
            </ds:Signature>
            <Subject>
              <!-- NameID indeholder en i organisationen unik ID for erhvervspersonen - kunne også
```

```
sættes til erhvervspersonens global unikke ID,
                som tildelt i den fællesoffentlige erhvervsadministration -->
                <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">KorsbaekKommune\MSK</NameID>
                <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
                   <SubjectConfirmationData xmlns:a="http://www.w3.org/2001/XMLSchema-
instance" a:type="KeyInfoConfirmationDataType">
                      <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                         <X509Data>
                            <!-- Holder-of-key certifikatet - dvs. certifikat for det system/SOSI-STS-klient som
kan veksle bootstraptokenet til et SOSI-idkort-->
                            <X509Certificate>MII ... xjQs</X509Certificate>
                         </X509Data>
                      </KeyInfo>
                   </SubjectConfirmationData>
                </SubjectConfirmation>
             </Subject>
             <Conditions NotOnOrAfter="2020-11-12T12:22:50.027Z">
                <!-- Aftageren som må omveksle dette bootstraptoken (her SOSI-STS'en)  -->
                <AudienceRestriction>
                   <Audience>https://sts.sosi.dk/</Audience>
                </AudienceRestriction>
             </Conditions>
             <AttributeStatement>
                <!-- Angivelse af profil og version (konstanten 'OIO-SAML-3.0') -->
                <Attribute Name="https://data.gov.dk/model/core/specVersion"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                   <AttributeValue>OIO-SAML-3.0</AttributeValue>
                </Attribute>
                <!-- Sikringsniveau udtrykt efter NSIS -->
                <Attribute Name="https://data.gov.dk/concept/core/nsis/loa"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                   <AttributeValue>Substantial</AttributeValue>
                </Attribute>
                <!-- Ervhvervspersonens global unikke ID, som tildelt i den fællesoffentlige
erhvervsadministration -->
                <Attribute Name="https://data.gov.dk/model/core/eid/professional/uuid/persistent"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                   <AttributeValue>urn:uuid:323e4567-e89b-12d3-a456-426655440000</AttributeValue>
                </Attribute>
                <!-- Organisationens CVR nummer (her Korsbæk Kommunes) -->
                <Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                   <AttributeValue>20301823</AttributeValue>
                </Attribute>
                <!-- Organisationens navn (her Korsbæk Kommune) -->
                <Attribute Name="https://data.gov.dk/model/core/eid/professional/orgName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                   <AttributeValue>Korsbæk Kommune</AttributeValue>
                </Attribute>
                      <!-- En (frivillig) angivelse af brugerens centralt trustede og lokalt
                   administrerede 'nationale roller' formatteret som OIOBPP 1.2 XML struktur og
                   indlejret i Base64 encoded form
                      <Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                         <AttributeValue>Bx23z ....</AttributeValue>
                      </Attribute>
                   Eksempel (i Base64 decoded form) for en bruger med tildelt 'national rolle'
                   'Plejehjemsassistent' i Korsbæk Kommune:

                   <bpp:PrivilegeList
                    xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
```

```
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
              <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:20301823">
                <Privilege>urn:dk:healthcare:national-federation-
role:code:41003:value:PlejeAssR3</Privilege>
              </PrivilegeGroup>
            </bpp:PrivilegeList>

          -->
                    </AttributeStatement>
                </Assertion>
            </wst14:ActAs>
            <wsp:AppliesTo>
                <wsa:EndpointReference>
                    <wsa:Address>https://fmk</wsa:Address>
                </wsa:EndpointReference>
            </wsp:AppliesTo>
            <wst:Claims Dialect="http://docs.oasis-
open.org/wsfed/authorization/200706/authclaims">

                <!-- Attribut som er påkrævet i SOSI idkortet og angives angives her som
claim -->
                <auth:ClaimType Uri="medcom:ITSystemName">
                    <auth:Value>Korsbæk Kommunes IT systemer</auth:Value>
                </auth:ClaimType>

                <!-- Frivillige attributter som kan anvendes fx til valg af sundhedsfaglig
autorisation (eller 'national rolle') -->
                <auth:ClaimType Uri="medcom:UserRole">
                    <!-- Uddannelseskode for 'Læge' -->
                    <auth:Value>7170</auth:Value>
                </auth:ClaimType>
                <!-- Eksempel med angivelse af national rolle 'Plejehjemsassistent'
                <auth:ClaimType Uri="medcom:UserRole">
                    <auth:Value>urn:dk:healthcare:national-federation-
role:code:41003:value:PlejeAssR3</auth:Value>
                </auth:ClaimType>
                -->
                <!-- Eksempel med angivelse af autorisations ID (fremfor
uddannelseskode)
                <auth:ClaimType Uri="medcom:UserAuthorizationCode">
                    <auth:Value>ZXCVB</auth:Value>
                </auth:ClaimType>
                -->
<!-- Eksempel med angivelse af ID som ønskes sat som Subject NameID i SOSI idkortet
<auth:ClaimType Uri="sosi:SubjectNameID">
    <auth:Value>Mads_Skjern</auth:Value>
</auth:ClaimType>
-->

            </wst:Claims>
        </wst:RequestSecurityToken>
    </soapenv:Body>
</soapenv:Envelope>
```

1.3.2.3. Eksempel BST2SOSI STS-response

Nedenfor vises et eksempel på et BST2SOSI retursvar med SOSI idkort, der matcher ovenstående BST2SOSI request.

```
<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wst="http://docs.oasis-
open.org/ws-sx/ws-trust/200512" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd">
   <soapenv:Header>
      <wsa:Action wsu:Id="action">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa:Action>
      <wsa:MessageID wsu:Id="messageID">urn:uuid:6b09a6eb-1539-4bbe-a367-
8d9d9c4b20f6</wsa:MessageID>
      <wsa:RelatesTo wsu:Id="relatesTo">urn:uuid:bfe03422-990c-49ec-9a31-
07eeb82ffed3</wsa:RelatesTo>
      <wsse:Security mustUnderstand="1" wsu:Id="security">
         <wsu:Timestamp wsu:Id="ts">
            <wsu:Created>2020-11-12T08:09:53Z</wsu:Created>
         </wsu:Timestamp>
         <ds:Signature>
            <ds:SignedInfo>
               <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
               <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <ds:Reference URI="#messageID">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>AubBTkl44/WOoYqN4JZg96Ks2qE=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference URI="#action">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>3cXAhlhZH22NiSh7AttxKxBap7Q=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference URI="#relatesTo">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>oe9O9MQRb9hFSIblLUns69YfAtU=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference URI="#ts">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>CF/Pjtr//fCqWISF0PS7DeEjBgI=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference URI="#body">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>pRDhdBP4vg21xhs3q7kIpdhjXE8=</ds:DigestValue>
               </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>ny ... Eg==</ds:SignatureValue>
            <ds:KeyInfo>
```

```
            <ds:X509Data>
               <ds:X509Certificate>MII ... FQ==</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
   </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="body">
   <wst:RequestSecurityTokenResponseCollection>
      <wst:RequestSecurityTokenResponse Context="urn:uuid:b216a8d9-0cab-40f7-8f60-
8fa854c284a7">
         <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
         <wst:RequestedSecurityToken>
            <!-- SOSI idkortet -->
            <saml:Assertion IssueInstant="2020-11-12T08:09:53Z" Version="2.0" id="IDCard">
               <saml:Issuer>TEST2-NSP-STS</saml:Issuer>
               <saml:Subject>
                  <saml:NameID Format="medcom:other">KorsbaekKommune\MSK</saml:NameID>
                  <saml:SubjectConfirmation>
                     <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key</saml:ConfirmationMethod>
                     <saml:SubjectConfirmationData>
                        <ds:KeyInfo>
                           <ds:KeyName>OCESSignature</ds:KeyName>
                        </ds:KeyInfo>
                     </saml:SubjectConfirmationData>
                  </saml:SubjectConfirmation>
               </saml:Subject>
               <saml:Conditions NotBefore="2020-11-12T08:04:53Z" NotOnOrAfter="2020-11-
13T08:04:53Z"/>
               <saml:AttributeStatement id="IDCardData">
                  <saml:Attribute Name="sosi:IDCardID">
                     <saml:AttributeValue>0gawKVevRYQ45IrGJt+r6w==</saml:AttributeValue>
                  </saml:Attribute>
                  <saml:Attribute Name="sosi:IDCardVersion">
                     <saml:AttributeValue>1.0.1</saml:AttributeValue>
                  </saml:Attribute>
                  <saml:Attribute Name="sosi:IDCardType">
                     <saml:AttributeValue>user</saml:AttributeValue>
                  </saml:Attribute>
                  <saml:Attribute Name="sosi:AuthenticationLevel">
                     <saml:AttributeValue>4</saml:AttributeValue>
                  </saml:Attribute>
               </saml:AttributeStatement>
               <saml:AttributeStatement id="UserLog">
                  <saml:Attribute Name="medcom:UserCivilRegistrationNumber">
                     <saml:AttributeValue>1802602810</saml:AttributeValue>
                  </saml:Attribute>
                  <saml:Attribute Name="medcom:UserGivenName">
                     <saml:AttributeValue>Mads</saml:AttributeValue>
                  </saml:Attribute>
                  <saml:Attribute Name="medcom:UserSurName">
                     <saml:AttributeValue>Skjern</saml:AttributeValue>
                  </saml:Attribute>
                  <saml:Attribute Name="medcom:UserRole">
                     <saml:AttributeValue>7170</saml:AttributeValue>
                  </saml:Attribute>
                  <saml:Attribute Name="medcom:UserAuthorizationCode">
                     <saml:AttributeValue>ZXCVB</saml:AttributeValue>
                  </saml:Attribute>
               </saml:AttributeStatement>
```

```
            <saml:AttributeStatement id="SystemLog">
               <saml:Attribute Name="medcom:ITSystemName">
                  <saml:AttributeValue>Korsbæk Kommunes IT systemer</saml:AttributeValue>
               </saml:Attribute>
               <saml:Attribute Name="medcom:CareProviderID"
NameFormat="medcom:cvrnumber">
                  <saml:AttributeValue>20301823</saml:AttributeValue>
               </saml:Attribute>
               <saml:Attribute Name="medcom:CareProviderName">
                  <saml:AttributeValue>Korsbæk Kommune</saml:AttributeValue>
               </saml:Attribute>
            </saml:AttributeStatement>
            <ds:Signature id="OCESSignature">
               <ds:SignedInfo>
                  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
                  <ds:Reference URI="#IDCard">
                     <ds:Transforms>
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                     </ds:Transforms>
                     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                     <ds:DigestValue>Fn9Dyi9gZTxaEOFyWmODqKB7rhE=</ds:DigestValue>
                  </ds:Reference>
               </ds:SignedInfo>
               <ds:SignatureValue>sQA ... rw==</ds:SignatureValue>
               <ds:KeyInfo>
                  <ds:X509Data>
                     <ds:X509Certificate>MII ... FQ==</ds:X509Certificate>
                  </ds:X509Data>
               </ds:KeyInfo>
            </ds:Signature>
         </saml:Assertion>
      </wst:RequestedSecurityToken>
      <wsp:AppliesTo>
         <wsa:EndpointReference>
            <wsa:Address>https://fmk</wsa:Address>
         </wsa:EndpointReference>
      </wsp:AppliesTo>
      <wst:Lifetime>
         <wsu:Created>2020-11-12T08:04:53Z</wsu:Created>
         <wsu:Expires>2020-11-13T08:04:53Z</wsu:Expires>
      </wst:Lifetime>
   </wst:RequestSecurityTokenResponse>
</wst:RequestSecurityTokenResponseCollection>
</soapenv:Body>
</soapenv:Envelope>
```