SUNDHEDSDATA-
STYRELSEN

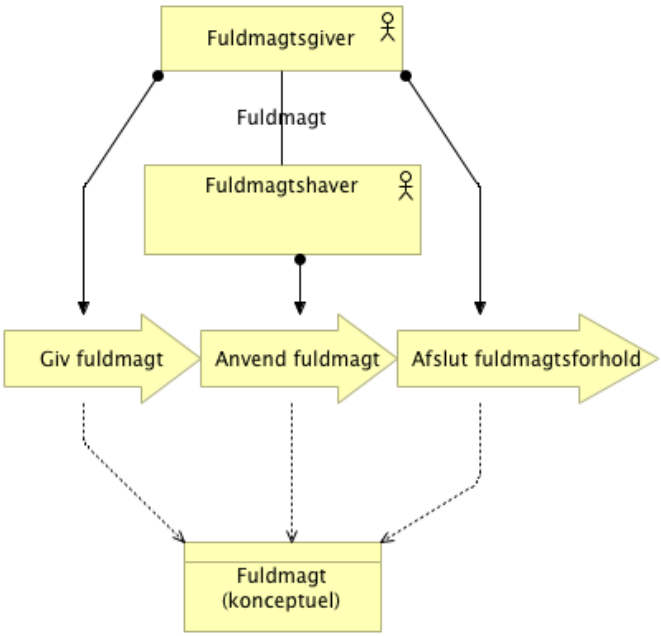
Sundhedsvæsenets anvendelse af den fællesoffentlige fuldmagtsservice.

Teknisk Løsningsbeskrivelse

Version	Dato	Ansvarlig	Kommentarer
0.2	04.04.2018	JRI	Dokument oprettet
0.3	05.04.2018	JRI	Indledning, overordnet arkitektur og teknisk setup beskrevet.
0.4	09.04.2018	Anni	Review
0.5	09.05.2018	JRI	CHG kommentarer samt XML indføjet.
0.6	18.06.2018	JRI	HEBL kommentarer indarbejdet.
1.0	25.06.2018	JRI	Opdateret XML indsat. Godkendt af HEBL.

Indledning

I takt med at digitaliseringen af sundhedsvæsenet øges med udbredelsen af digitale tjenester som f.eks. “Fælles Medicinkort” og digital understøttelse af “Tværgående Komplekse Forløb”, bliver det i stigende grad vigtigt, at borgere, der har berøring med sundhedsvæsenet, kan give fuldmagt så f.eks. pårørende eller nærtstående kan støtte borgeren på vejen gennem sundhedsvæsenet.
Fuldmagter er relationer mellem borgere (borger-til-borger). Et klassisk eksempel på en digital fuldmagt er en person, der ikke føler sig tryg ved digitale løsninger, der giver fuldmagt til sin søn eller datter, så datteren kan agere på vegne af forælderen. Foruden at udpege de to parter i fuldmagten, indeholder fuldmagten typisk også informationer, der indskrænker fuldmagten i tid og genstandsfelt, så der f.eks. give fuldmagt til at se eller agere på et bestemt område i en bestemt periode.



Figur 1 - Konceptuel illustration af de væsentligste processer, aktører og forretningsobjekter.

Den borgervendte understøttelse af digitale fuldmagter eksisterer allerede i den fællesoffentlige NemLog-in infrastruktur. NemLog-in fuldmagtsløsningen består af:

- En brugergrænseflade på Borger.dk hvor borgeren kan give, ændre og nedlægge fuldmagter
- En teknisk snitflade hvor særlige tjenester kan anmode om fuldmagtsoplysninger for en given befuldmægtiget
- En integration til den tekniske snitflade fra NemLog-in’s Identity Provider (IdP) og NemLog-in’s Security Token Service (STS), så

fuldmagtsinformationer indlejres i de tekniske ”tokens”, der udstedes af IdP’en og STS’en og kan anvendes i adgangsstyring til offentlige digitale services

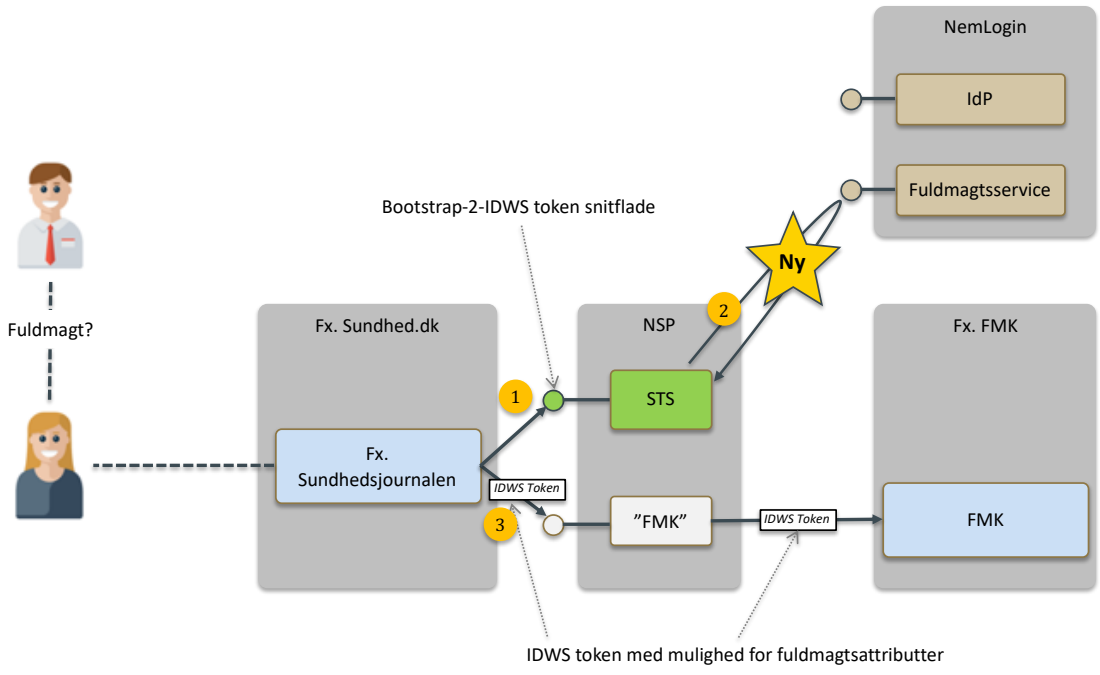
I forbindelse med videreudviklingen af de nationale services[1] er det blevet aktuelt og relevant at få indarbejdet fuldmagtsmuligheder i de borgervendte services **på sundhedsområdet**. Fra FMK app’en til mobilen og fra de borgervendte brugergrænseflade hos Sundhed.dk og FMK online er der i den forbindelse behov for at kalde bagvedliggende services, (FMK-servicen og Stamkortsservicen på Komplekse forløb) som igen har behov for at få informationer fra autoritative kilder om fuldmagtsforhold mellem borgere. Disse informationer overføres på sundhedsområdet via security-tokens (IDWS tokens) udstedt af den nationale Security Token Service (SOSI STS).

Nærværende løsning består derfor i at få udvidet den nuværende IDWS snitflade på sundhedsvæsenets nationale STS (SOSI STS’en) til at kunne verificere ’claims’ om afgivet fuldmagt ved at kontrollere at et påstået fuldmagtsforhold rent faktisk eksisterer i NemLog-in’s fuldmagtsregister.

[1] Konkret Fælles medicinkort (FMK) og introduktionen af Tværgående Komplekse Forløb

Overordnet arkitektur

Når en borger ønsker at repræsentere en anden borger (fuldmagtsgiver) i relation til f.eks. FMK eller Komplekse Tværgående Forløb, er det et arkitekturmæssigt princip, at de bagvedliggende services ikke selv skal forestå verificering af påståede fuldmagtsrelationer, men kan "stole" på et udsagn fra en troværdig komponent, der har foretaget verifikationen forud for serviceanmodningen.
Konkret er det på sundhedsområdet NSP'ens "Security Token Service" (SOSI-STS), der verificerer fuldmagter og kommunikerer fuldmagten gennem de udstedte "tokens".
Løsningen består i sin enkelthed af en verifikation af et claim i STS'en ved hjælp af en webservice hos NemLog-ins fuldmangtsservice. Claim'et er kun til stede og skal kun verificeres, når en borger ønsker at være partsrepræsentant for en anden borger. Løsningen benytter kun én operation på NemLogin fuldmagtsservicen ("getDelegation") og integrationen sker kun fra den STS operation, hvor en borgers "bootstrap token" omveksles til et IDWS token ("Bootstrap-2-IDWS").
Løsningens logiske komponenter og integrationer er illustreret nedenfor:



Figur 2 - Der skabes en ny integration fra SOSI-STS til NemLogin Fuldmagtsservicen mhp. at backendsystemer kan lade borgere partsrepræsentere en fuldmagtsgiver. Backend services (her FMK) kan kontrollere fuldmagtsforhold alene ved at inspicere det medsendte IDWS token.

Som det ses af illustrationen ovenfor, skaffes IDWS tokenet (1+2) forud for serviceanvendelsen (3). Afhængig af anvender-løsningen (FMK appen, Sundhedsjournalen mv.) vil det være lidt forskelligt hvor på brugerrejsen, IDWS tokenet skabes, og hvorledes de nødvendige parameterinformationer opsamles. Fælles for alle anvendelser gælder det dog, at der i forespørgslen om udstedelse af IDWS token skal medsendes et "claim" til STS'en som lidt forsimplet indeholder "ønske om verifikation af fuldmagt til løsning X fra fuldmagtsgiver Y til fuldmagtshaver Z". I IDWS tokenet vil der efter verifikation være informationer i retningen af "der er verificeret fuldmagt mellem fuldmagtsgiver X til fuldmagtshaver Y for løsning Z".

IDWS tokens med fuldmagtsinformationer

Løsningen ændrer kun på indholdet af "BST2IDWS" snitfladen på STS'en (WS-TRUST / SOAP). Her følger nogle eksempler på, hvorledes XML-strukturen i det store hele bliver påvirket:

WS trust request med fuldmagts claims:

```
<?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#" xml
ns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:wsa="http://www.w3.org/2005/08/a
ddressing" 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:1c2818b8-9ab3-4898-9730-
dab518020b05</wsa:MessageID>
    <wsse:Security mustUnderstand="1" wsu:Id="security">
      <wsu:Timestamp wsu:Id="ts"><wsu:Created>2018-05-
24T09:17:40Z</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:Reference>
          <ds:Reference URI="#action"> ...</ds:Reference>
          <ds:Reference URI="#ts">...</ds:Reference>
          <ds:Reference URI="#body">...</ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
                <!-- FOCES certifikat i base64-encodet form til signering af -->
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="body">
    <wst:RequestSecurityToken Context="urn:uuid:f637dd3e-fad4-4f5e-ac55-baa504560772">
      <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>
          <!-- nemlogin bootstrap token in cleartext -->
```

```
        </saml:Assertion>
      </wst14:ActAs>
      <wsp:AppliesTo>
        <wsa:EndpointReference>
          <wsa:Address>http://audience/clear</wsa:Address>
        </wsa:EndpointReference>
      </wsp:AppliesTo>
      <wst:Claims Dialect="http://docs.oasis-
open.org/wsfed/authorization/200706/authclaims">
        <auth:ClaimType Uri="dk:gov:saml:attribute:CprNumberIdentifier">
          <auth:Value>0501792275</auth:Value>
        </auth:ClaimType>
        <auth:ClaimType Uri="dk:healthcare:saml:attribute:OnBehalfOf">
          <auth:Value>urn:dk:healthcare:saml:actThroughProcurationBy:cprNumberIdentifi
er:1111111118</auth:Value>
        </auth:ClaimType>
      </wst:Claims>
    </wst:RequestSecurityToken>
  </soapenv:Body>
</soapenv:Envelope>
```

Ovenstående vil give anledning til følgende kald til den fællesoffentlige fuldmagtsservice:

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
    <soap:Body>
        <GetDelegations xmlns="https://DelegationQuery.Nemlog-in.dk/"

xmlns:ns2="http://schemas.datacontract.org/2004/07/DK.OES.KFOBS.Delegation.Frontend.De
legationWebService"
 xmlns:ns3="http://schemas.microsoft.com/2003/10/Serialization/"

xmlns:ns4="http://schemas.datacontract.org/2004/07/DK.OES.KFOBS.FBRS.Common.Contracts"
>
            <entityId>entitydummy</entityId>
            <representativeId>
                <ns2:PID>PID:9208-2002-2-514358910503</ns2:PID>
            </representativeId>
        </GetDelegations>
    </soap:Body>
</soap:Envelope>
```

og følgende svar fra den fællesoffentlige fuldmagtsservice (dummy):

```
<?xml version="1.0" encoding="UTF-8" ?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
    <soap:Body>
        <GetDelegationsResponse xmlns="https://DelegationQuery.Nemlog-in.dk/"

xmlns:ns2="http://schemas.datacontract.org/2004/07/DK.OES.KFOBS.Delegation.Frontend.De
legationWebService"

xmlns:ns3="http://schemas.microsoft.com/2003/10/Serialization/"

xmlns:ns4="http://schemas.datacontract.org/2004/07/DK.OES.KFOBS.FBRS.Common.Contracts"
>
            <GetDelegationsResult>
                <ns2:Delegations>
                    <ns2:Delegation>
                        <ns2:CitizenCpr>1111111118</ns2:CitizenCpr>
                        <ns2:Privileges>
                            <ns2:string>read</ns2:string>
                        </ns2:Privileges>
                    </ns2:Delegation>
                    <ns2:Delegation>
                        <ns2:CitizenCpr>0101603040</ns2:CitizenCpr>
                        <ns2:Privileges>
                            <ns2:string>write</ns2:string>
                        </ns2:Privileges>
                    </ns2:Delegation>
```

```
            </ns2:Delegations>
            <ns2:ResponseId>PID:9208-2002-2-514358910503</ns2:ResponseId>
        </GetDelegationsResult>
    </GetDelegationsResponse>
  </soap:Body>
</soap:Envelope>
```

Herefter vil STS'en filtrere i disse svar og returnere et svar der minder om flg.

```
<?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/polic
y" 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:b032de90-34a1-44dc-95ce-
8b5a61bcf592</wsa:MessageID>
    <wsa:RelatesTo wsu:Id="relatesTo">urn:uuid:04a6576e-607e-4edc-8b6c-
aaa26d75f2d6</wsa:RelatesTo>
    <wsse:Security mustUnderstand="1" wsu:Id="security">
      <wsu:Timestamp wsu:Id="ts">
        <wsu:Created>2018-05-24T09:37:49Z</wsu:Created>
      </wsu:Timestamp>
      <ds:Signature> <!- response er signeret med STS certifikat -->
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="body">
    <wst:RequestSecurityTokenResponseCollection>
      <wst:RequestSecurityTokenResponse Context="urn:uuid:d1126e37-5ebf-4fd6-bbd7-
67c8063509bf">
        <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
        <wst:RequestedSecurityToken>
          <saml:Assertion
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchem
a-instance" ID="_0eac8d61-a226-4a85-97c0-8d5a5a964178" IssueInstant="2018-05-
24T09:37:49Z" Version="2.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="
urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:Issuer>TESTSTS</saml:Issuer>
            <ds:Signature Id="OCESSignature">
              <!-- assertion signeret af STS -->
            </ds:Signature>
            <saml:Subject>
              <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=Ingen organisatorisk tilknytning,CN=Lars
Larsen,Serial=PID:9208-2002-2-514358910503</saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-
of-key">
              <saml:SubjectConfirmationData NotOnOrAfter="2018-05-
24T09:42:48Z" Recipient="http://audience/clear">
                <ds:KeyInfo>
                  <ds:X509Data>
                    <ds:X509Certificate>MIIGIjCCBQqgAwIBAgIEWBjCxjANBgkqhkiG9w0BAQsF
ADBHMQswCQYDVQQGEwJESzESMBAGA1UECgwJVFJVU1QyNDA4MSQwIgYDVQQDDBtUUlVTVDI0MDggU3lzdGVtdG
VzdCBYSVggQ0EwHhcNMTcwMTMwMDcwNjQ3WhcNMjAwMTMwMDcwNjE0WjCBkDELMAkGA1UEBhMCREsxJzAlBgNV
BAoMHk5FVFMgREFOSUQgQS9TIC8vIENWUjozMDgwODQ2MDFYMCAGA1UEBRMZQ1ZSOjMwODA4NDYwLUZJRDo5ND
czMTMxNTA0BgNVBAMMLVRVIEdFTkVSRUwgRk9DRVMgZ3lsZGlnIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANLzkWLn7qgPVpNZFIpq2X7kUR00IPreIF6osVsdAXWAs61/1m
AFr7jMklEOTe9f/2iddZ77SlWhvnsWWnU3y0P9jnKrNnQh6VRo/ykqgKK/wCXMAuHBsZJ9yJ8XuZ6MhDEbY/kt
SdSpvCqmoz3eBYLp7fqewNcjMg69hbGW5V+EPmurM4z1+HN+CAKjeyjYnoqwOcENdXJZ8Ctx1Rnwy1UWZizzav
HnN0XZzVj+MmT4yVE/SXDRhDwhsR/CEa4ghFWGqG+bCOIh8Q2axZgYaUtLkpb8syYOlPpxq2ow/ZoZAlpctCw9
kbbacxPyUH7GT62qzdJbNVnGb6HE49J++gUCAwEAAaOCAsowggLGMA4GA1UdDwEB/wQEAwIDuDCBlwYIKwYBBQ
UHAQEEgYowgYcwPAYIKwYBBQUHMAGGMGh0dHA6Ly9vY3NwLnN5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3Jl
c3BvbmRlcjBHBggrBgEFBQcwAoY7aHR0cDovL2YuYWlhLnN5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3N5c3
RlbXRlc3QxOS1jYS5jZXIwggEgBgNVHSAEggEXMIIBEzCCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUH
AgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA4LmNvbS9yZXBvc2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRD
ADAgEBGoGrRGFuSUQgdGVzdCBjZXJ0aWZpa2F0ZXIgZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAx
LjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuIERhbklEIHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQS
BhcmUgaXNzdWVkIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuMIGqBgNVHR8EgaIwgZ8w
PKA6oDiGNmh0dHA6Ly9jcmwuc3lzdGVtdGVzdDE5LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDE5LmNybDBfoF
```

```
2gW6RZMFcxCzAJBgNVBAYTAkRLMRIwEAYDVQQKDAlUUlVTVDI0MDgxJDAiBgNVBAMMG1RSVVNUMjQwOCBTeXN0
ZW10ZXN0IFhJWCBDQTEOMAwGA1UEAwwFQ1JMOTYwHwYDVR0jBBgwFoAUzAJVDOSBdK8gVNURFFeckVI4f6AwHQ
YDVR0OBBYEFM87NIlSfKvNYR6xTrPPLlP5/zDaMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQELBQADggEBAHJ4gA73
YkRR4BaFgcbi5BRCtYUqxdr0Ip6Hx/yY9+PZv9YvnhnLTvCRTs18oJK8lGlTL/lAeQfCM/CAo9V/4e6IhhbUYa
ehmAguR+4uSMrJXyThvB/6aOYLsdyPwpBmXSaBXbCjVIpUgZ7Q6FemhUuslTNsy3Tt/zDfAgqHhlLjB33io9hY
OefT9/IIFkJ32pa5itni0yNzOUi1jC4tx8XdOZGN17lBkXtmaGWh9grWd17x3odVG+kYoa+TekdKOys8bY7ZQw
kqktJZnitMgQmbtuGHHQ+9ZXeEwZhhL/U+Lda3O92m8HSdgiHRhvoZ4+j3e/PbRaUW2z5YSqBoua4=</ds:X50
9Certificate>
                    </ds:X509Data>
                  </ds:KeyInfo>
                </saml:SubjectConfirmationData>
              </saml:SubjectConfirmation>
            </saml:Subject>
            <saml:Conditions NotBefore="2018-05-24T09:32:48Z" NotOnOrAfter="2018-05-
24T09:42:48Z">
              <saml:AudienceRestriction>
                <saml:Audience>http://audience/clear</saml:Audience>
              </saml:AudienceRestriction>
            </saml:Conditions>
            <saml:AttributeStatement>
              <saml:Attribute
Name="dk:gov:saml:attribute:SpecVer" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                <saml:AttributeValue xsi:type="xs:string">DK-SAML-
2.0</saml:AttributeValue>
              </saml:Attribute>
              <saml:Attribute
Name="dk:gov:saml:attribute:AssuranceLevel" NameFormat="urn:oasis:names:tc:SAML:2.0:at
trname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">3</saml:AttributeValue>
              </saml:Attribute>
              <saml:Attribute
Name="dk:gov:saml:attribute:CprNumberIdentifier" NameFormat="urn:oasis:names:tc:SAML:2
.0:attrname-format:basic">
                <saml:AttributeValue
xsi:type="xs:string">0501792275</saml:AttributeValue>
              </saml:Attribute>
              <saml:Attribute
Name="dk:gov:saml:attribute:Privileges_intermediate" NameFormat="urn:oasis:names:tc:SA
ML:2.0:attrname-format:basic">
                <saml:AttributeValue xsi:type="xs:string">
                   <!-- fuldmagts privilegier i Base64 encodet form -->
                </saml:AttributeValue>
              </saml:Attribute>
            </saml:AttributeStatement>
          </saml:Assertion>
        </wst:RequestedSecurityToken>
        <wsp:AppliesTo>
          <wsa:EndpointReference>
            <wsa:Address>http://audience/clear</wsa:Address>
          </wsa:EndpointReference>
        </wsp:AppliesTo>
        <wst:Lifetime>
          <wsu:Created>2018-05-24T09:32:48Z</wsu:Created>
          <wsu:Expires>2018-05-24T09:42:48Z</wsu:Expires>
        </wst:Lifetime>
      </wst:RequestSecurityTokenResponse>
    </wst:RequestSecurityTokenResponseCollection>
  </soapenv:Body>
</soapenv:Envelope>
```

Privileges_intermediate attributten er base64-enkodet udgave af følgende indhold:

```
<?xml version="1.0" encoding="UTF-8" ?>
<bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile">
  <bpp:PrivilegeGroup
Scope="urn:dk:healthcare:saml:actThroughProcurationBy:cprNumberIdentifier:1111111118">
    <bpp:Privilege>urn:dk:nspop:sts:fmk:read</bpp:Privilege>
    <bpp:Privilege>urn:dk:nspop:sts:fmk:write</bpp:Privilege>
    <bpp:Privilege>urn:dk:nspop:sts:fsk:read</bpp:Privilege>
    <bpp:Privilege>urn:dk:nspop:sts:fsk:write</bpp:Privilege>
  </bpp:PrivilegeGroup>
```

```
</bpp:PrivilegeList>
```

Link til eksemplerne: https://www.nspop.dk/display/STS/SOAP+eksempler

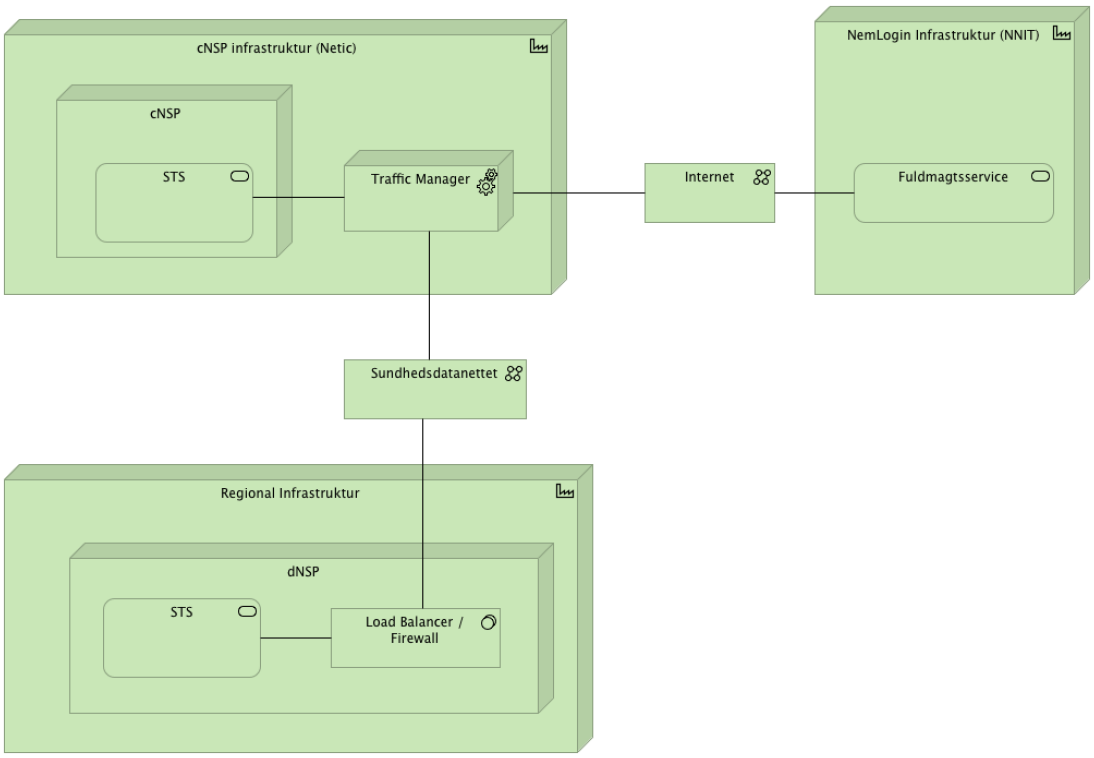
Teknisk setup

Der skabes en ny integration fra NSP'ernes STS komponent til den fællesoffentlige fuldmagtsløsning. Når en borger ønsker at repræsentere en anden borger (og kun i disse tilfælde!) verificerer STS'en at der findes en fuldmagtsrelation af den rette type mellem de to borgere. Hvis verifikationen enten ikke kan gennemføres eller viser, at der ikke findes den fornødne fuldmagtsrelation, skal STS'en returnere med en fejl til klientsystemet. Integrationen etableres som en on-line integration, dvs. der skabes ikke caches, lokale synkroniserede databaser eller lignende i denne løsning.

Omvekslingen fra OIOSAML bootstrap-token til et IDWS service token med fuldmagtsattributter skal kunne ske på alle STS'er i NSP. Der er dog en lille udfordring i dette, idet ét af NSP principperne tilsiger, at dNSP'erne ikke må have adgang (skal beskyttes fra) internettet, mens fuldmagtsservicen hos NemLog-in netop (og kun) er tilgængelig via internettet. En tilsvarende situation var man i, da STS'en oprindeligt skulle integreres med RID-til-CPR tjenesten hos NemID. På daværende tidspunkt blev det besluttet, at route disse kald ind over cNSP driftsleverandørens infrastruktur. Det forventer vi også at gøre i denne løsning (se Figur 3). Konsekvensen af dette er desværre, at et andet af NSP principperne, nemlig princippet om at have færrest mulige centrale fejlpunkter i infrastrukturen, ikke kan opretholdes. Denne afvejning er aftalt med SDS arkitekturfunktionen.

Arkitekturmæssigt følger kravene til denne udvidelse de generelle krav til STS-komponenten. Da der ikke caches eller på anden vis opbevares runtime-data til denne del af løsningen, er der pt. ingen krav til disaster recovery etc. Løsningen skal naturligvis logge fejl mv. jf. husreglerne for NSP så denne del af STS'en også bliver passende overvåget.

Bortset fra dette, er løsningen teknisk set relativt simpel, idet STS'erne blot kobles op på NemLog-in's web service. Det er dog meget vigtigt, at STS koden programmeres "defensivt" så fuldmagtsservice kaldet kun udføres ved relevante vekslingskald, samt at der indbygges gode og robuste værn mod, at fuldmagtsservicen eller netværket hen til fuldmagtsservicen er utilgængelig eller meget langsom. Det ville være ideelt, om øvrige STS'kald kunne prioriteres højere end disse fuldmagtservice omvekslinger, idet denne type omvekslinger må formodes at være mindre væsentlige end f.eks. de sundhedsfagliges autentifikations-forespørgsler.



Figur 3 - Alle STS'er integreres med NemLog-in fuldmagtsservicen, men alle integrationer er nødsaget til at gå gennem cNSP driftsleverandørens infrastruktur for at beskytte dNSP'erne fra internettet.