DIGITALISERINGSSTYRELSEN

NemLog-in

Teknisk guide til integration med Digital Fuldmagt

Indholdsfortegnelse

Ændringslog 2
1 Om denne guide 3
2 Baggrund og motivation 4
3 Afgrænsninger 5
4 Arkitektur og sammenhæng 6
5 Overblik over myndighedens opgaver 7
5.1 Web SSO grænseflade 7
6 Web Service snitflader 9
6.1 Metoden GetDelegations 9
6.2 Metoden GetDelegationsCreatedByCitizen 12
6.3 Metoden GetAllCreatedDelegationsAssignedToItSystem 14
7 Andre tekniske forhold 19
7.1 Udløb og tilbagekaldelser af fuldmagt 19
7.2 Logning 19
7.3 Brugerstyring 19
7.4 Test af løsningen 20
8 Tilpasning af brugergrænseflade 21
9 Håndtering af papirfuldmagter 22
10 Overvejelser om ressourceindsats 23
11 Referencer 24

Ændringslog

Dato	Version	Ændringsbeskrivelse	Initialer
18.11.2021	1.0	Formatering af guide samt teksttilpasninger	TG/LEASA

1 Om denne guide

Denne guide beskriver, hvorledes man som tjenesteudbyder (myndighed eller it-leverandør) kan integrere en offentlig borgerrettet løsning til NemLog-in's fuldmagtsløsning (Digital Fuldmagt). Guiden er henvendt til teknisk-orienterede personer, der skal planlægge eller udføre integrationen, og den beskriver de relevante aktiviteter, samt de snitflader, som anvendes i integrationen.

Yderligere information om fuldmagtsløsningen findes på NemLog-ins supportsite: https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/digital-fuldmagt/hjaelp-og-vejledning/

Læseren antages at være bekendt med basal terminologi inden for føderationer og brugerstyring.

2 Baggrund og motivation

Siden 2013 har den digitale fuldmagtsløsning planlagt været en selvstændig komponent i NemLog-in. Løsningen gør det muligt for borgere at give en fuldmagt til en repræsentant, således at repræsentanten kan agere på borgerens vegne i de offentlige selvbetjeningsløsninger, der er tilsluttet Digital Fuldmagt. Fuldmagter kan gives til andre borgere, en medarbejder i en virksomhed eller en virksomhed (via CVR nummer).

Digital Fuldmagt er en fællesoffentlig komponent, som indebærer en række fordele for de involverede parter:

- Myndigheder får mulighed for at understøtte fuldmagter i deres borgerrettede it-løsninger uden selv at skulle bygge en applikation til administration af fuldmagter. Dermed vil arbejdet med at understøtte digitale fuldmagter blive væsentligt reduceret, og myndighederne får mulighed for at begrænse brugen af de "analoge" kanaler.
- Myndigheder kan i høj grad genbruge de snitflader, der i forvejen anvendes til integration mod NemLog-in og fællesoffentlig brugerstyring, herunder OIOSAML.
- Borgere får mulighed for på en kontrolleret måde at give adgang til en repræsentant til at udføre handlinger på deres vegne – uden at være fristet til at videregive deres NemID kodeord og nøglekort, hvilket er en usikker praksis i strid med reglerne.
- Borgerne får én samlet indgang til at administrere deres fuldmagter til offentlige selvbetjeningsløsninger, og det bliver muligt at give fuldmagter som dækker flere myndighedsløsninger på én gang.
- Det bliver lettere for repræsentanter at anmode samt anvende fuldmagter fra borgere på en konsistent måde på tværs af myndigheder.
- Brugen af fuldmagter (processer, terminologi, brugergrænseflade, teknik mv.) harmoniseres på tværs af den offentlige sektor i takt med at fuldmagtsløsningen tages i anvendelse af myndighederne. Videreudvikling af fuldmagtsløsningen kommer alle parter til gode.

3 Afgrænsninger

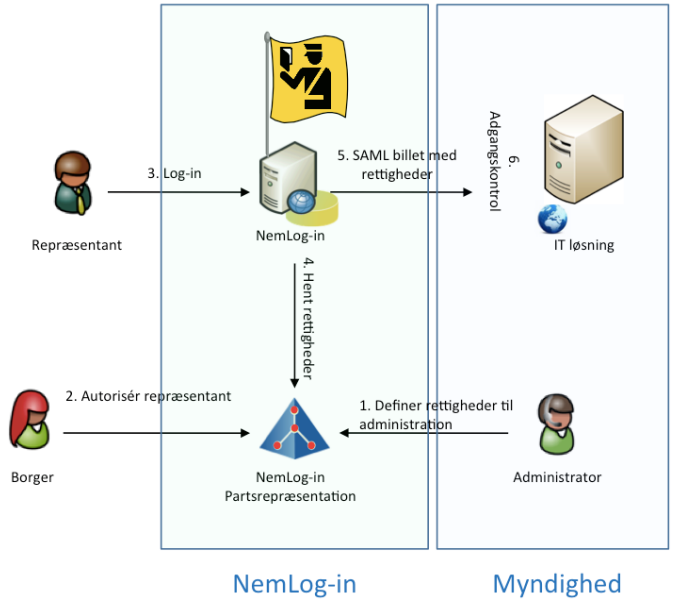
NemLog-in's fuldmagtsløsning er afgrænset til at håndtere digitale fuldmagter, der kan udtrykkes som delegering af rettigheder til it-systemer, der er tilsluttet NemLog-in. Dette indebærer en række fordele, idet denne type anvendelse kan opnå en høj grad af digitalisering med bl.a. automatisk fortolkning af fuldmagtens indhold, mens der omvendt findes en række scenarier for fuldmagter, som ikke kan håndteres - herunder fuldmagter med 'fritekst', der skal fortolkes af personer, eller fuldmagter som ikke vedrører it-systemer tilsluttet NemLog-in.

NemLog-in's fuldmagtsløsning kan endvidere kun anvendes af offentlige myndigheder i deres selvbetjeningsløsninger.

4 Arkitektur og sammenhæng

Digital Fuldmagt er designet med henblik på, at myndighedsløsninger skal ændres så lidt som muligt for at kunne understøtte digitale fuldmagter. Det antages således, at myndighedsløsninger i forvejen anvender NemLog-in til autentifikation af borgere til løsningen. Dette vil konkret ske via OIOSAML snitfladen, hvor NemLog-in udsteder en SAML Assertion (billet) til myndighedsløsningen, der rummer information om brugerens identitet mv.

Denne integration genbruges i fuldmagtsløsningen således, at når der er givet en digital fuldmagt, da vil brugerens SAML Assertion blive udvidet med et antal fuldmagtsprivilegier (rettigheder), som formidler dels *hvem* der er modtaget fuldmagt fra og dels *hvilken adgang*, der er givet.



1. Myndighedens administrator opretter et antal fuldmagtsprivilegier for sin løsning i NemLog-in Administrationen, der svarer til delegérbare adgange i myndighedens løsning.
2. En borger opretter en fuldmagt via brugergrænsefladen i Digital Fuldmagt, der delegerer en rettighed (fuldmagtsprivilegie) til en repræsentant.
3. Repræsentanten logger ind på myndighedsløsningen via NemLog-in.
4. NemLog-in detekterer ved opslag i fuldmagtsdatabasen, at brugeren (repræsentanten) har modtaget en fuldmagt fra en borger.
5. NemLog-in sender en SAML Assertion til myndighedsløsningen, som dels rummer information om brugerens (repræsentantens) identitet og dels rummer information om de fuldmagter, brugeren har modtaget til løsningen.
6. Myndighedsløsningen detekterer at brugeren, der logger ind, har fuldmagt til at agere på andre borgeres vegne. Fuldmagtsprivilegierne anvendes i løsningens adgangskontrol, således at de rette adgange opnås, og brugeren bliver i brugergrænsefladen spurgt, hvem han vil agere på vegne af (sig selv eller andre).

Løsningen understøtter også andre varianter end ovenstående scenarie, eksempelvis hvor fuldmagter hentes via API og således ikke er tæt koblet til repræsentantens log-in.

5 Overblik over myndighedens opgaver

Hvis en myndighed ønsker at benytte fuldmagtsløsningen, er der en række tekniske opgaver, der skal udføres:

1. Myndigheden skal tilslutte sin løsning til NemLog-in, således at brugerne logger ind via denne. Et stort antal myndigheder er i forvejen tilsluttet NemLog-in. Er dette tilfældet, kan denne aktivitet overspringes.
2. Myndigheden skal definere de fuldmagtsprivilegier (delegérbare rettigheder) for deres løsning, som skal kan kunne gives fra borgere til repræsentanter. Privilegierne er løsningsspecifikke, så myndigheden kan frit vælge, hvorledes disse designes.
3. Fuldmagtsprivilegierne skal oprettes i NemLog-in via NemLog-in Administrationen samt gives en udførlig beskrivelse, så borgere forstår implikationerne af at delegere dem til en repræsentant.
4. Myndigheden skal udvide sit brugerstyringsmodul i egen selvbetjeningsløsning, så rettighederne modtaget i SAML billetter fra NemLog-in giver repræsentanten adgang til de relevante dele af myndighedsløsningen.
5. Myndigheden skal etablere den nødvendige logning, så der sikres dokumentation for, hvad repræsentanten foretager på borgerens vegne i myndighedsløsningen.
6. Myndigheden skal opdatere brugergrænsefladen i sin løsning, så repræsentanten dels kan vælge, hvem han vil agere på vegne af og efterfølgende tydeligt kan se, hvem han aktuelt repræsenterer.

OBS: Det er vigtigt at myndigheden opsætter fuldmagten således, at fx mindreårige ikke kan pådrage sig et erstatnings eller strafferetsligt ansvar på baggrund af sine handlinger med en fuldmagt i løsningen.

5.1 Web SSO grænseflade

Som nævnt ovenfor kan OIOSAML grænsefladen anvendes til integration mellem NemLog-in og myndighedens løsning. Dette betyder, at myndighedsløsninger som i forvejen anvender NemLog-in til log-in formål, ikke behøver at integrere til nogle nye snitflader for at anvende fuldmagtsløsningen.

Når en bruger logger på myndighedsløsningen via NemLog-in, vil NemLog-in udstede en SAML Assertion til myndighedsløsningen med information om brugeren. I forbindelse med behandling af den modtagne SAML Assertion skal myndighedsløsningen tage højde for to nye forhold:

a) Den modtagne SAML Assertion kan angive, at brugeren har fået delegeret fuldmagtsprivilegier til løsningen på vegne af borgere (se nedenfor).

b) For borgerrettede selvbetjeningsløsninger er der formentlig behov for at kunne tillade log-in for professionelle (med medarbejdercertifikater), som repræsenterer borgere via fuldmagtsprivilegier. Når en bruger logger på NemLog-in med et medarbejdercertifikat, vil NemLog-in medsende nogle andre attributter til myndighedsløsningen[1] – konkret vil SAML billetten ikke indeholde et PID/UUID[2] og CPR nummer hørende til en personidentitet, men i stedet et CVR og RID/UUID nummer hørende til en

[1] Se [OIO-SAML] for detaljer.

[2] Med overgangen fra OIOSAML 2 til 3 erstattes PID- og RID-numre generelt med UUID'er entydig reference til identiteten.

medarbejderidentitet. Hvis myndighedsløsningen er programmeret til altid at kræve et PID/UUID eller CPR nummer, vil den således skulle udvides.

Syntaksen for indlejring af privilegier i SAML Assertions er defineret i OIOSAML Basic Privilege Profile [OIO-BPP]. Her angives fuldmagtsprivilegiet ved den tilhørende URI, som myndigheden har indmeldt til NemLog-in. Brugerens privilegier er angivet i attributten `https://data.gov.dk/model/core/eid/privilegesIntermediate` i den udstedte OIO SAML 3.0 Assertion[3].

Et eksempel på denne:

```
<saml:Attribute FriendlyName="Privileges"
   Name=" https://data.gov.dk/model/core/eid/privilegesIntermediate"
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
   <saml:AttributeValue xsi:type="xs:string">
      <base64 encoded value>
   </saml:AttributeValue>
```

Værdien af attributten er en base64 indkodet streng, der kan dekodes til en XML struktur, som indeholder en liste af privilegier:

```
<?xml version="1.0" encoding="UTF-8"?>
<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:cprNumberIdentifier:2001692832">
       <Privilege>urn:dk:some_domain:myPrivilege1A</Privilege>
       <Privilege>urn:dk:some_domain:myPrivilege1B</Privilege>
```

Scope attributten på PrivilegeGroup elementet angiver den kontekst (afgrænsning), som gælder for de tildelte privilegier (repræsenteret ved Privilege elementer), der er indlejret. Fuldmagtsprivilegier er kendetegnet ved, at scope er sat til et CPR nummer, der identificerer fuldmagtsgiver. I ovenstående eksempel er der således delegeret fuldmagtsprivilegierne myPrivilege1A og myPrivilege1B på vegne af CPR nummer *2001692832*, og fuldmagtsprivilegierne myPrivilege1C og myPrivilege1D på vegne af CPR nummer *1102871829*.

Hvis et konkret scope ikke understøttes af løsningen, kan man ignorere rettigheden og/eller give brugeren en fejlmeddelelse.

[3] I OIOSAML 2 profilerne har attributten et andet navn.

6 Web Service snitflader

En myndighedsløsning vil normalt få formidlet en fuldmagt via den SAML Assertion, der udstedes til brugeren/repræsentanten ved log-in (se ovenfor). Som alternativ udstiller NemLog-in SOAP-baserede web service grænseflader, hvor fuldmagtsprivilegier kan *forespørges* (det er ikke muligt at oprette fuldmagter på denne måde). Man vælger hvilken af de to metoder (evt. begge), der skal anvendes for ens løsning, via afkrydsning i NemLog-in/Administration.

Web service grænsefladerne har den fordel, at det er muligt at forespørge om fuldmagtsprivilegier for en vilkårlig bruger (repræsentant) eller for en organisation, mens Web SSO grænsefladen kun formidler fuldmagtsprivilegier tildelt den aktuelle bruger, som logger ind. Dette kan eksempelvis anvendes ved integration til tjenesteudbyderens interne systemer som f.eks. i kundeportaler eller andet, hvor en sagsbehandler eller supportmedarbejder kan have behov for at vide, om der foreligger en fuldmagt, uden at repræsentanten nødvendigvis er logget ind på selvbetjeningsløsningen (eksempelvis hvis repræsentanten henvender sig via andre kanaler som telefon eller e-mail, og sagsbehandleren skal kontrollere, om der foreligger et fuldmagtsforhold ift. henvendelsen).

Nedenfor gennemgås kort de forskellige metoder på web servicen.

Servicen er beskyttet af to-vejs TLS dvs. myndighedsløsningen skal anvende et klientcertifikat (OCES Funktionscertifikat eller Virksomhedscertifikat), der forinden er registreret til myndighedens it-system (EntityID). Registreringen af certifikatet sker via NemLogin Administrationen. Certifikatet kan enten være det samme, som anvendes i forbindelse med signering og kryptering af SAML meddelelser (som i angivet i SAML metadatafilen) eller et helt separat certifikat.

6.1 Metoden GetDelegations

Metoden `GetDelegations` returnerer fuldmagter for en specifik repræsentant. Den tager flg. input:

- `EntityID` på myndighedsløsningen (som angivet løsningens SAML metadatafil, der uploaded til NemLog-in)
- `ID` på repræsentant, som der forespørges fuldmagter på: dette kan enten være CVR+RID for en repræsentant, et CPR nummer eller PID nummer for et borgercertifikat.

Herunder findes et eksempel på et SOAP request, hvor der forespørges på fuldmagter til en medarbejderrepræsentant:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">

  <s:Header>

    <Action s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">

https://DelegationQuery.Nemlog-in.dk/IQueryWebService/GetDelegations</Action>

  </s:Header>

  <s:Body>

    <GetDelegations xmlns="https://DelegationQuery.Nemlog-in.dk/">

      <entityId>http://entityid16.dk</entityId>

      <representativeId xmlns:d4p1="http://schemas.datacontract.org/2004/07/

DK.OES.KFOBS.Delegation.Frontend.DelegationWebService"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

        <d4p1:CVR>15731249</d4p1:CVR>

        <d4p1:PID i:nil="true" />

        <d4p1:CPR i:nil="true" />
```

Web servicen returnerer et svar med følgende elementer:

- Et response id
- En liste med delegeringer

Response id er en entydig værdi beregnet til logningsformål. Med denne er det muligt at korrelere logninger på tværs af myndighedsløsningen og NemLog-in.

Et eksempel på SOAP Response:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">

  <s:Header>

    <ActivityId CorrelationId="bb24ed05-0086-4685-b54b-e286ed937b00"
xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">

f2e02326-9cdc-475d-904c-a130227a1923</ActivityId>

  </s:Header>

  <s:Body>

    <GetDelegationsResponse xmlns="https://DelegationQuery.Nemlog-in.dk/">

      <GetDelegationsResult xmlns:a="http://schemas.datacontract.org/2004/07/

DK.OES.KFOBS.Delegation.Frontend.DelegationWebService"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

        <a:Delegations>

          <a:Delegation>

            <a:CitizenCpr>1015731249</a:CitizenCpr>

            <a:Privileges
xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays">

              <b:string>http://acme.org/privilege1</b:string>

              <b:string>http://acme.org/privilege2</b:string>

              <b:string>http://acme.org/privilege3</b:string>

            </a:Privileges>

          </a:Delegation>
```

Bemærk at der kun udstedes privilegier hørende til løsningens EntityID. Det er således ikke muligt at forespørge på fuldmagter givet til andre løsninger, dvs. hverken løsninger inden for samme myndighed eller løsninger fra andre myndigheder.

Den præcise snitflade (WSDL fil) findes på NemLog-ins supportsite for tjenesteudbydere[4] i sektionen 'Opsætning af webservice kald'.

[4] https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/digital-fuldmagt/hjaelp-og-vejledning/

6.2 Metoden GetDelegationsCreatedByCitizen

Denne mode returnerer en liste over alle fuldmagter (aktive og ikke-aktive) oprettet af en borger til en bestemt service. Det forretningsmæssige formål med metoden er at understøtte supportsituationer ved henvendelser fra borger eller repræsentant, hvor der er behov for at afklare status på afgivne fuldmagter - herunder om de evt. måtte være udløbet eller tilbagetrukket.

Metoden tager følgende input:

- `entityId` på myndighedsløsningen (som angivet løsningens SAML metadatafil, der uploaded til NemLog-in)
- `citizenId` på den borger, hvis fuldmagter der forespørges på: dette kan enten være et CPR nummer eller PID nummer for et borgercertifikat.

Eksempel på et SOAP request, hvor der forespørges på fuldmagter til en medarbejderrepræsentant:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">

  <s:Header>

    <Action s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">https://Delegati
onQuery.Nemlog-in.dk/IQueryWebService/GetDelegationsCreatedByCitizen</Action>

  </s:Header>

  <s:Body>

    <GetDelegationsCreatedByCitizen xmlns="https://DelegationQuery.Nemlog-
in.dk/">

      <entityId>https://saml.wsp1c.ph</entityId>

      <citizenId
xmlns:d4p1="http://schemas.datacontract.org/2004/07/DK.OES.KFOBS.Delegation.Fron
tend.DelegationWebService" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

        <d4p1:Cpr>2011501190</d4p1:Cpr>

        <d4p1:Pid i:nil="true" />

      </citizenId>
```

Web servicen returnerer et svar med følgende elementer:

- Et response id (til korrelerings- og logningsformål)
- En liste med fuldmagter (delegeringer) som indeholder
    - Repræsentant (borger, medarbejder, organisation)
    - Oprettelsesdato
    - Udløbsdato
    - Status (aktiv, udløbet, tilbagekaldt)
    - Navn på fuldmagten

- Fuldmagtsprivilegier i fuldmagten for det pågældende it-system (identificeret ved EntityID)

Eksempel på svar fra servicen:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">

  <s:Header />

  <s:Body>

    <GetDelegationsCreatedByCitizenResponse
xmlns="https://DelegationQuery.Nemlog-in.dk/">

      <GetDelegationsCreatedByCitizenResult
xmlns:a="http://schemas.datacontract.org/2004/07/DK.OES.KFOBS.Delegation.Fronten
d.DelegationWebService" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

        <a:Delegations>

          <a:Delegation i:type="a:DelegationExt">

            <a:Privileges>

              <a:string>https://delegation.ph</a:string>

            </a:Privileges>

            <a:Representative i:type="a:citizen">

              <a:CPR>1111111111</a:CPR>

            </a:Representative>

            <a:DateCreated>2015-08-14T08:23:02.593</a:DateCreated>

            <a:Expiration>2015-10-14T21:59:59</a:Expiration>

            <a:Status>Aktiv</a:Status>

            <a:DelegationName>citizen priv auto 1|Del priv WSP
1</a:DelegationName>

          </a:Delegation>

          <a:Delegation i:type="a:DelegationExt">

            <a:Privileges>

              <a:string>https://delegation.ph</a:string>

            </a:Privileges>

            <a:Representative i:type="a:organization">

              <a:CVR>10213231</a:CVR>

              <a:CVRName>Økonomistyrelsen</a:CVRName>

            </a:Representative>

            <a:DateCreated>2015-08-14T08:31:46.277</a:DateCreated>

            <a:Expiration>2015-10-14T21:59:59</a:Expiration>
```

6.3 Metoden GetAllCreatedDelegationsAssignedToItSystem

Denne metode returnerer en liste over alle aktive borgerfuldmagter til en service. Metoden kan benyttes ved massebehandling af sager, hvor servicen har behov for at vide hvilke borgere, der har oprettet en fuldmagt. Dette kan fx være relevant, hvis servicen skal udsende information til både borgeren og dennes repræsentant.

Metoden tager følgende input:

- entityID på myndighedsløsningen (som angivet løsningens SAML metadatafil, der uploaded til NemLog-in)
- privilegeUri, navn på privilege fx. urn:dk:umit:minsu:privilege_grants
- offset* parameter. Denne skal have værdien 0 ved første kald til servicen. Hvis der er flere fuldmagter registreret end der maksimalt tillades returneret per kald, så benyttes denne parameter til at hente the resterende fuldmagter

* Der kan potentiel være mange fuldmagter der skal returneres til servicen. Webservicen har en max grænse på antal fuldmagter, der returneres per kald. Hvis der er flere fuldmagter end max grænsen, så skal offset parameteren benyttes ved efterfølgende kald til at hente alle fuldmagter (dette er illustreret senere med et kodeeksempel senere i dette afsnit).

Eksempel på et SOAP request:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">

  <s:Header>

    <Action s:mustUnderstand="1"
xmlns="http://schemas.microsoft.com/ws/2005/05/addressing/none">https://DelegationQuery.Nemlog-
in.dk/IQueryWebService/GetAllCreatedDelegationsAssignedToItSystem</Action>

  </s:Header>

  <s:Body>

    <GetAllCreatedDelegationsAssignedToItSystem xmlns="https://DelegationQuery.Nemlog-in.dk/">

      <entityId>https://saml.it17.dmz.test</entityId>

      <privilegeUri>https://saml.it17.dmz.test/sys17Delegationprivilege1</privilegeUri>

      <offset>0</offset>

    </GetAllCreatedDelegationsAssignedToItSystem>

  </s:Body>

</s:Envelope>
```

Webservicen returnerer et svar med flg. elementer:

- Et response id (til korrelerings- og logningsformål)
- En liste med fuldmagter (delegeringer) som indeholder
  - CPR nummer på borgeren
  - Repræsentant (borger, medarbejder, organisation)
  - Udløbsdato
- Antal fuldmagter returneret
- Total antal fuldmagter
- Næste offset værdi – hvis denne værdi er større end nul, så skal webservicen kaldes igen med denne offset værdi som input.

Eksempel på svar fra servicen:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">

  <s:Header />

  <s:Body>

    <GetAllCreatedDelegationsAssignedToItSystemResponse xmlns="https://DelegationQuery.Nemlog-
in.dk/">

      <GetAllCreatedDelegationsAssignedToItSystemResult
xmlns:a="http://schemas.datacontract.org/2004/07/DK.OES.KFOBS.Delegation.Frontend.DelegationWebS
ervice" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

        <a:Delegations>

          <a:Delegation i:type="a:DelegationExt">

            <a:CitizenCpr>1506492984</a:CitizenCpr>

            <a:Privileges i:nil="true" />

            <a:Representative i:type="a:citizen">

              <a:CPR>3005761503</a:CPR>

            </a:Representative>

            <a:Expiration>2016-08-08T21:59:59</a:Expiration>

          </a:Delegation>

          <a:Delegation i:type="a:DelegationExt">

            <a:CitizenCpr>1506492984</a:CitizenCpr>

            <a:Privileges i:nil="true" />

            <a:Representative i:type="a:citizen">

              <a:CPR>2506042049</a:CPR>

            </a:Representative>
```

```
      <a:Expiration>2016-08-09T21:59:59</a:Expiration>
    </a:Delegation>
    <a:Delegation i:type="a:DelegationExt">
      <a:CitizenCpr>2506042049</a:CitizenCpr>
      <a:Privileges i:nil="true" />
      <a:Representative i:type="a:citizen">
        <a:CPR>0606163958</a:CPR>
      </a:Representative>
      <a:Expiration>2016-08-10T21:59:59</a:Expiration>
    </a:Delegation>
    <a:Delegation i:type="a:DelegationExt">
      <a:CitizenCpr>3005761503</a:CitizenCpr>
      <a:Privileges i:nil="true" />
      <a:Representative i:type="a:organization">
        <a:CVR>10213231</a:CVR>
      </a:Representative>
      <a:Expiration>2016-08-22T21:59:59</a:Expiration>
    </a:Delegation>
    <a:Delegation i:type="a:DelegationExt">
      <a:CitizenCpr>1106550779</a:CitizenCpr>
      <a:Privileges i:nil="true" />
      <a:Representative i:type="a:organization">
        <a:CVR>10213231</a:CVR>
      </a:Representative>
      <a:Expiration>2016-09-04T21:59:59</a:Expiration>
    </a:Delegation>
    <a:Delegation i:type="a:DelegationExt">
      <a:CitizenCpr>0306140246</a:CitizenCpr>
      <a:Privileges i:nil="true" />
      <a:Representative i:type="a:organization">
        <a:CVR>10213231</a:CVR>
      </a:Representative>
      <a:Expiration>2016-10-08T21:59:59</a:Expiration>
```

```
          </a:Delegation>
          <a:Delegation i:type="a:DelegationExt">
            <a:CitizenCpr>0306140246</a:CitizenCpr>
            <a:Privileges i:nil="true" />
            <a:Representative i:type="a:employee">
              <a:CVR>10213231</a:CVR>
              <a:RID>75817932</a:RID>
              <a:PersonName>Svend Sørensen</a:PersonName>
            </a:Representative>
            <a:Expiration>2016-10-08T21:59:59</a:Expiration>
          </a:Delegation>
        </a:Delegations>
        <a:ResponseId>1cae8f6f-34c9-45c5-8fdc-552de63e6081</a:ResponseId>
        <a:NextOffset>-1</a:NextOffset>
        <a:NumberOfRecordsReturned>7</a:NumberOfRecordsReturned>
        <a:TotalNumberOfRecords>7</a:TotalNumberOfRecords>
      </GetAllCreatedDelegationsAssignedToItSystemResult>
    </GetAllCreatedDelegationsAssignedToItSystemResponse>
  </s:Body>
</s:Envelope>
```

Følgende kodeeksempel i C# illustrerer, hvordan webservicen skal kaldes ved brug af et loop pattern for at sikre at alle fuldmagter returneres.

```
List<QueryWebService.Delegation> delegations = new List<QueryWebService.Delegation>();

//loop through the method to get all records until there is nothing to fetch anymore
(until the returned nextOffset = 0)

int offset = 0; //start at offset 0

int nextOffset = 0;

do

{

    // call service

    var delegationResponse = client.GetAllCreatedDelegationsAssignedToItSystem(entityId,

        privilegeUrl, offset);

    // add result to list

    delegations.AddRange(delegationResponse.Delegations);

    // get the next offset value

    nextOffset = delegationResponse.NextOffset;

    offset = nextOffset;

} while (nextOffset > 0);
```

7 Andre tekniske forhold

Uanset hvilken snitflade, der anvendes til integration med fuldmagtsløsningen, er der en række tekniske forhold, som skal overvejes og håndteres af myndighedens løsning.

7.1 Udløb og tilbagekaldelser af fuldmagt

Fuldmagter kan til enhver tid tilbagetrækkes af borgeren, der har udstedt den. Når repræsentanten logger på myndighedsløsningen, vil kun fuldmagtsprivilegier hørende til aktive fuldmagter på log-in-tidspunktet blive medtaget i den udstedte SAML Assertion, men derudover er der ingen mekanismer, hvormed fuldmagtsløsningen kan formidle til myndighedsløsninger, at en fuldmagt er tilbagetrukket.

Derfor skal myndighedsløsninger følge den konvention, at fuldmagter kun anvendes i den aktuelle browsersession, hvor repræsentanten er logget ind - men ikke anvendes i efterfølgende browsersessioner. Desuden bør sessioner nedlægges efter 30 minutters inaktivitet i henhold til NemLog-in's timeoutpolitik. Det er således vurderet som værende tilstrækkeligt, at fuldmagten er gyldig på det tidspunkt, hvor repræsentanten logger ind, når disse forhold iagttages.

Et lignende aspekt er knyttet til udløb af fuldmagter. En fuldmagt har altid en udløbsdato angivet af fuldmagtsgiver. Hvis repræsentanten logger på en myndighedsløsning kort før midnat, kan man i princippet risikere, at fuldmagten anvendes på en senere dato end SAML Assertion er udstedt, hvor den potentielt ikke længere er gyldig. Myndigheder skal derfor at detektere datoskift i deres sessionshåndtering og i givet fald foretage fornyet log-in af brugeren via NemLog-in for at konstatere, om fuldmagten stadig er aktiv (dvs. om fuldmagtsprivilegierne stadig er til stede i den gen-udstedte SAML Assertion). Bemærk i den forbindelse at hvis repræsentanten stadig har en session med NemLog-in, da vil dette log-in ske uden det er nødvendigt at afgive kodeord (med andre ord et passivt log-in). Det vil derfor ikke være til unødig gene for repræsentanten.

7.2 Logning

Myndigheden skal udvide sin logning, så flg. forhold klart dokumenteres:

a) Når en repræsentant logger ind med fuldmagtsprivilegier
b) Hvilke handlinger en repræsentant udfører på vegne af borgere

De detaljerede krav til logningen er angivet i NemLog-in's logningspolitik[5].

7.3 Brugerstyring

I mange borgerrettede myndighedsløsningen opereres der med en simpel rettighedsmodel, idet alle borgere typisk må foretage de samme *handlinger* i løsningen – men kun på deres egne data. Der er altså tale om en rettighedsmodel baseret på dataafgrænsninger frem for funktionelle afgrænsninger. For sådanne løsninger har der typisk ikke været brug for at definere eksplicitte rettigheder, som kunne tildeles brugerne.

Dette forhold kan ændre sig med introduktion af fuldmagter, idet repræsentanter typisk skal kunne delegeres adgang til specifikke dele af en myndighedsløsning. Hvis der således er behov for mere end ét fuldmagtsprivilegie til en myndighedsløsning, er det nødvendigt at udvide

[5] https://www.nemlog-in.dk/tu/krav/logningspolitik

rettighedsmodellen, så repræsentanter kun får den korrekte, afgrænsede adgang. Hvorledes dette nemmest implementeres i myndighedsløsningen afhænger af de konkrete forhold. I nogle løsninger kan det være enklest at udforme nogle særlige skærmbilleder, som kun anvendes af repræsentanter, mens man i andre i løsninger kan genanvende de skærmbilleder, som i forvejen anvendes af borgere, og hvor man så frakobler de funktioner, der ikke måtte være omfattet af den givne fuldmagt.

7.4 Test af løsningen

I forbindelse med udvikling af tilpasningerne til myndighedsløsningen, er det naturlige forløb først at teste integrationen mod NemLog-in's integrationstestmiljø, og når denne fungerer, gå videre til produktionsmiljøet. Her er det relevant at bemærke, at brugergrænsefladen til NemLog-in's fuldmagtsløsning, hvor fuldmagter administreres, findes kun i en produktionsudgave. Derimod kan NemLog-in's integrationstestmiljø godt udstede SAML Assertions indeholdende fuldmagtsprivilegier.

I NemLog-in Administrationen er det således muligt at tildele nogle fuldmagtsprivilegier til testbrugere i integrationstestmiljøet, som den enkelte myndighed selv definerer. Ved efterfølgende at logge ind med disse testbrugere på myndighedsløsningen, kan man se hvordan SAML Assertions med fuldmagtsprivilegier behandles, herunder at repræsentanter får de korrekte adgange i myndighedsløsningen.

8 Tilpasning af brugergrænseflade

Som tidligere nævnt vil der være behov for at tilpasse brugergrænsefladen i myndighedsløsningen. Formålet med interaktionsdesignet er at sikre en konsistent brugeroplevelse på tværs af løsninger i den offentlige sektor, hvilke også bidrager til brugeres genkendelse og gør, at brugerne føler sig mere sikre i anvendelse af løsningen. Nedenfor en liste over de tilpasninger som kan være relevante:

- Når en repræsentant logger ind med fuldmagtsprivilegier for en eller flere borgere, skal vedkommende vælge hvilken person, repræsentanten (slutbrugeren) aktuelt ønsker at repræsentere. Som repræsentant bør det kun være muligt at kunne agere som én person ad gangen (evt. sig selv).
- For at repræsentanten altid kan være sikker på, hvilken person vedkommende handler på vegne af, skal det tydeligt og konstant angives i brugergrænsefladen, når repræsentanten udfører handlinger på vegne af en anden borger. Det anbefales desuden en tydelig bekræftelse på vigtige handlinger, hvor repræsentanten skal godkende handlingen. Ligeledes bør det være muligt at skifte bruger.
- Brugergrænsefladen bør afspejle rettighederne i den fuldmagt, som er givet. Hvis det er muligt at give fuldmagt til dele af applikationen, bør de dele/funktioner, hvortil der ikke foreligger fuldmagt, ikke kunne vælges af repræsentanten.
- Man kan overveje, om det skal fremgå i brugergrænsefladen, hvilke handlinger, der er foretaget af en repræsentant via fuldmagt. Desuden kan man overveje, om det er relevant at sende kvitteringer for vigtige handlinger, som er blevet foretaget af en repræsentant på borgerens vegne til borgerens digitale postkasse.
- Hjælpetekster og brugervejledninger skal udvides til at beskrive mulighederne for fuldmagt.
- Løsningen skal rumme mulighed for navigering til fuldmagtsløsningen – via en knap eller link med titlen ”Giv fuldmagt”. Der er pt. to alternative muligheder for dette:
    - Myndighedsløsningen kan integrere fuldmagtsløsningen på sin egen web side via iFraming integration. Herved undgår man, at borgeren skal forlade myndighedsløsningen for at afgive fuldmagt, og listen over mulige fuldmagtsprivilegier kan blive filtreret til kun at vise dem, der er relevante for løsningen.
    - Alternativt kan man linke til fuldmagtsløsningen, således at denne åbner som en selvstændig applikation i browseren.

9 Håndtering af papirfuldmagter

Det spiller ingen rolle for integrationen til myndighedsløsningen, hvordan en digital fuldmagt er tilvejebragt dvs. hvad enten den er indtastet af borgeren selv eller af en betroet medarbejder i den myndighed, som ejer en offentlig løsning, der er tilsluttet til Digital Fuldmagt. Fuldmagtsprivilegier fremgår på helt samme måde i den udstedte SAML Assertion samt via API'er.

Hvis myndigheden vælger at modtage papirfuldmagter fra borgere, som indtastes af betroede medarbejdere, sker dette via den brugergrænseflade, som Digital Fuldmagt stiller til rådighed. Der er derfor ingen opgaver for myndighedsløsningen i den forbindelse. Dog skal de pågældende medarbejdere forinden have udstedt et OCES medarbejdercertifikat og blive udpeget som betroede medarbejdere via NemLog-in/Brugeradministration af myndighedens administrator. Dette står yderligere beskrevet i vejledningen "Sådan hjælper I borgere med at oprette fuldmagt" som kan findes på: https://digst.dk/it-loesninger/digital-fuldmagt/vejledninger/

10 Overvejelser om ressourceindsats

Nedenfor gives nogle overslag på den forventede indsats ved tilpasning af en myndighedsløsning, som skal anvende fuldmagtsløsningen, når denne i forvejen er tilsluttet NemLog-in.

Det skal understreges, at indsatsen vil variere med kompleksiteten og teknologien i myndighedsløsningen, samt desuden med udviklernes viden om brugerstyring. For nuværende findes ingen erfaringsbaserede tal at bygge på, men i takt med at erfaringer indsamles, vil estimaterne blive opdateret. Derfor skal estimaterne anvendes med et vist forbehold.

1. Definition af fuldmagtsprivilegier og oprettelse i NemLog-in: 4 – 8 timer
2. Udvidelse af adgangskontrolmodul: 15 – 60 timer
3. Udvidelse af logning: 10 – 20 timer
4. Tilpasning af brugergrænseflade: 30 – 60 timer
5. Test af udvidelserne: 20 – 40 timer

Dertil kommer diverse projektoverhead i form af planlægning, projektledelse, afklaringer, kommunikation, dokumentation etc.

11 Referencer

[OIO-SAML] ”OIO Web SSO Profile V3.0.2”, Digitaliseringsstyrelsen.

https://digst.dk/it-loesninger/nemlog-in/anvendelse/oiosaml-302/

[OIO-BPP] ”OIO Basic Privilege Profile”, Digitaliseringsstyrelsen.
https://digst.dk/it-loesninger/nemlog-in/anvendelse/oiosaml-302/