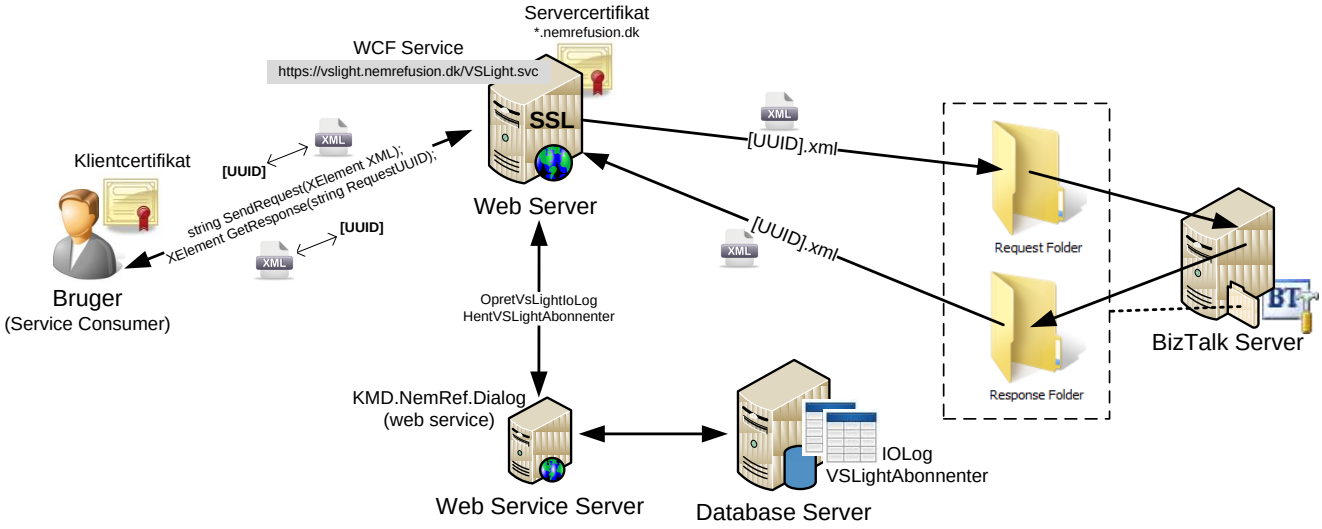
NemRefusion VSLight – Systemdokumentation

Virksomhedsservice via webservice

Dette dokument beskriver implementeringen af VSLight i NemRefusion. Med VSLight kan virksomheder integrere til NemRefusion virksomhedsservice via en webservice (WCF) i stedet for at bruge MQ. Dette dokument beskriver kun webservice-delen af løsningen, og altså ikke hvordan BizTalk behandler beskederne.



1 Kildekode

Løsningen ligger i en Visual Studio 2010 (.NET Framework 3.5) solution som kan findes i Subversion under:

`/svn/NemRefusion/trunk/VisualStudio/KMD.NemRefusion.VSLight`

Den indeholder to projekter:

1. **KMD.NemRefusion.VSLight**
   Hovedprojektet i form af en "WCF Service Application".
2. **KMD.NemRefusion.VSLightConsumeDemo**
   Hvis servicen er installeret efter installationsvejledningen kan den testes med denne "Console Application".

Koden er grundigt dokumenteret med XML kommentarer (///) og yderligere kommentarer inde i metoderne hvor nødvendigt.

2 Overordnet beskrivelse

VSLight er en sikker (https/SSL + påkrævet "registreret" klientcertifikat) webservice (WCF) som udstiller to metoder:

- string **SendRequest**(XElement XML); *"læg på kø"*
- XElement **GetResponse**(string RequestUUID); *"hent fra kø"*

VSLight erstatter kun selve MQ-kommunikationen, så det er stadig en forudsætning, at brugeren kan danne en gyldig NemRefusion XML besked (NemRefusionIndberetningSamling, NemRefusionVirksomhedSoegningStruktur, HaendelseSoegningStruktur eller SagsbehandlingSoegningStruktur) og korrekt påføre en XML signatur (XMLDsig).

Interfacet er typeløst for den transporterede XML så der kan ligesom på en kø kommunikeres enhver form for gyldig XML.

1. Med metodekaldet ***SendRequest*** giver brugeren som input sin XML, og output er et UUID som skal benyttes ved senere afhentning af svaret fra BizTalk.
2. Den leverede XML gemmes på et share, som BizTalk holder øje med, i en fil med filnavn som det returnerede UUID. (f0e2b7cd-d38c-443e-b07e-0f892b8a2bd7.xml)
3. BizTalk samler indberetningen op, behandler den, og lægger svaret i en XML fil med samme navn som input filen.
4. Brugeren kan ikke, som på en kø, se hvilke filer der ligger klar til afhentning, men må i stedet efter et passende stykke tid forsøge at hente det svar, der forhåbentlig vil ligge klar. Med et kald til metoden ***GetResponse*** gives som input et tidligere modtaget UUID, og som output fås XML beskeden i et .NET *XElement* objekt som direkte kan behandles eller gemmes til en fil på disken.
   a. Hvis metoden returnerer ***null*** så har servicen ikke kunne finde en XML fil med svaret fra BizTalk. Dette kan betyde at forespørgslen ikke er behandlet færdig endnu (eller er stallet) og brugeren må prøve igen lidt senere. Alternativt kan denne returværdi betyde, at det UUID der medsendes er forkert og altså aldrig har været returneret fra et kald til *SendRequest*,

eller det kan betyde at kaldet til *GetResponse* er foretaget for sent og filen med svaret er blevet ryddet op (slettet eller arkiveret).

2.1 Servers

Det er planen at selve servicen skal hostes på virksomhedsdialog serveren og ligge som et separat website ved siden af dialogen og tilslutningsløsningen. Til ekstra sikkerhedsfeatures og logning skal der kommunikeres med databasen, og til dette formål benytter servicen sig af dialogservicen på web service serveren på samme måde som virksomhedsdialogen gør det (se installationsvejledningen for mere information).

De to delte mapper som bruges til kommunikationen mellem VSLight og BizTalk er placeret på BizTalk serveren og skal være opsat til deling sådan, at brugeren for VSLights *application pool* har skriveadgang. For mappen med svar fra BizTalk skal der også være opsat en form for skemalagt oprydning sådan at filer der er ældre end en grænseværdi bliver slettet eller arkiveret.

3 Sikkerhed

Ud over den sikkerhed som i forvejen eksisterer i systemet, hvor den indsendte XML besked skal være signeret med et gyldigt virksomhedscertifikat, er der lagt yderligere sikkerhed ved kommunikation med VSLight servicen.

Servicen er sikret delvist ved opsætning på IIS og delvist i kode. IIS opsætningen (se installationsvejledning) leverer krypteret trafik over https/SSL og påkræver at brugeren identificerer sig med et klientcertifikat på transportniveau ved samtlige kald til servicen. På denne måde kan brugeren kun få kontakt hvis klientcertifikatet er udsted af en certifikatautoritet som webserveren stoler på (det samme rodcertifikat skal ligge i serverens certifikatlager).

Endvidere kan der kun kommunikeres succesfuldt med servicen hvis klientcertifikatets thumbprint er registreret i tabellen *VSLightAbonnenter* i NemRefusion databasen. Opslaget i databasen foretages via dialogservicen med metoden *HentVSLightAbonnenter* som returnerer listen over alle abonnenter. Abonnentkontrollen foregår i en "*custom certificate validator*" som der henvises til fra den tilhørende *service behavior* i web.config filen. Dette betyder at metoden *Validate* i klassen *ClientCertificateValidator* er det første der kaldes efter at IIS'en har godkendt certifikatet. Denne metode kaster en fejl hvis det kaldende certifikats thumbprint ikke er at finde blandt abonnenterne.

```
<behaviors>
  <serviceBehaviors>
    <behavior name="KMD.NemRefusion.VSLight.VSLightBehavior">
      <!-- Der tillades kun https kald. -->
      <serviceMetadata httpGetEnabled="false" httpsGetEnabled="true" />
      <serviceDebug includeExceptionDetailInFaults="false" />
      <serviceCredentials>
        <clientCertificate>
          <!-- Her bruges en hjemmelavet certifikat validator. -->
          <authentication certificateValidationMode="Custom"
            customCertificateValidatorType="KMD.NemRefusion.VSLight.ClientCertificateValidator, KMD.NemRefusion.VSLight"/>
        </clientCertificate>
      </serviceCredentials>
    </behavior>
  </serviceBehaviors>
</behaviors>
```

Alle former for kald til VSLight med ugyldigt eller manglende klientcertifikat vil modtage fejlbeskeden:

```
The HTTP request was forbidden with client authentication scheme 'Anonymous'.
```

I web.config filen findes også servicens *binding*, som ud over at forvente klientcertifikat på transporten også begrænser størrelsen på input (dette gælder XML input for *SendRequest*) til 10MB for at undgå overbelastning.

```
<basicHttpBinding>
  <!-- En basicHttpBinding til VSLight servicen som angiver at der forventes et klientcertifikat på transportniveau. -->
  <!-- Inputstørrelse begrænses til 10MB for ikke at overbelaste serveren. 1000 indberetninger ~ 5-6MB. -->
  <binding name="KMD.NemRefusion.VSLight.VSLightBinding" maxReceivedMessageSize="10000000">
    <security mode="Transport">
      <transport clientCredentialType="Certificate" />
    </security>
  </binding>
```

4 Logning

Ved hjælp den nye metode *OpretVsLightIoLog* i dialogservicen foretages grundig logning af fejl og IO. Til dette formål er der oprettet en ny tilhørende aktørtype (13/"VSLight") i databasen. Ved hver skrivning til IOLog registreres altid information om tidspunkter, aktørtype, og indberetter. *IndberetterIdentifikator* i loggen indeholder information om brugerens certifikat på formen:

```
CN=DANID A/S - DanID Test + SERIALNUMBER=CVR:30808460-UID:1237552804997, O=DANID A/S //
            CVR:30808460, C=DK; 4754015A500650873CBCB4D6BC6C604546BF6E8F
```

I de efterfølgende eksempler vises kun de supplerende kerneinformationer i logningen.

4.1 IO

Ved succesfuldt kald til metoden *SendRequest* logges navnet på rodelementet i den afleverede XML og værdien for den returnerede UUID.

IOType	Request	RequestUUID	Response	ResponseUUID
string SendRequest(XElement XML);	NemRefusionIndberetningSamling	NULL	[UUID]	84A94650-9E68-49BB-914A-73405721D773

Ved succesfuldt kald til metoden *GetResponse* logges værdien på det afleverede UUID og navnet på rodelementet i den returnerede XML, hvis det blev fundet, ellers logges værdien "[null]".

IOType	Request	RequestUUID	Response	ResponseUUID
XElement GetResponse(string RequestUUID);	NULL	74A94650-9E68-49BB-914A-73405721D773	[null]	NULL
XElement GetResponse(string RequestUUID);	NULL	84A94650-9E68-49BB-914A-73405721D773	NemRefusionIndberetningSamling	NULL

4.2 Fejl

Da der på IIS niveau sørges for at klientcertifikatet er gyldigt og betroet kan fejlforsøg af denne slags ikke bliver logget af VSLight.

Hvis klientcertifikatet slipper igennem IIS'en men ikke er på listen over abonnenter vil servicekalderen stadig modtage samme fejlbesked omkring "anonymous access" men hændelsen vil blive skrevet til loggen.

IOType	Requ...	Requ...	Res...	Res...	FejlKode	FejlTekst
NULL	NULL	NULL	NULL	NULL	102	User with client certificate thumbprint 4754015A500650873CBCB4D6BC6C604546BF6E8F is not a registered subscriber.
NULL	NULL	NULL	NULL	NULL	102	User with client certificate thumbprint 4754015A500650873CBCB4D6BC6C604546BF6E8F is not a registered subscriber.

Gyldigt input til metoden *GetResponse* er en UUID, men typen er kun begrænset til en tekststreng og kan derfor være ugyldig. I da fald modtager servicekalderen fejlbeskeden (System.ServiceModel.FaultException)

```
RequestUUID does not contain a valid UUID. (Example: 98f44b5b-5a45-4ad9-b13e-4b9366e5c01f)
```

Tilsvarende skrives i IOLog.

IOType	Request	RequestUUID	Response	ResponseUUID	FejlKode	FejlTekst
XElement GetResponse(string RequestUUID);	NULL	NULL	NULL	NULL	101	Invalid RequestUUID: abc123

Hvis servicen har problemer med at læse eller skrive i de to delte mapper, som bruges til kommunikationen med BizTalk modtages fejlbeskederne:

```
Request XML could not be delivered to an underlying system. Please try again later.
```

```
Response XML could not be acquired from an underlying system. Please try again later.
```

Detaljerne skrives til IOLog.

IOType	R	R	R	F	FejlKode	FejlTekst
XElement GetResponse(string RequestUUID);	N	N	N	I	104	Could not find a part of the path '\\172.30.58.202\virksomhedssystem2\VSLIGHTXXX'.
string SendRequest(XElement XML);	N	N	N	I	103	Could not find a part of the path '\\172.30.58.202\virksomhedssystem\VSLIGHTXXX\55fc87e4-4316-495b-a824-f71fb19cb38f.xml'.
XElement GetResponse(string RequestUUID);	N	N	N	I	104	The network name cannot be found.
string SendRequest(XElement XML);	N	N	N	I	103	The network name cannot be found.

5 Konfiguration

VSLight har tre vigtige konfigurationspunkter i form at stierne til BizTalk udvekslingsmapperne, referencen til dialogservicen og registreringen af abonnenter.

5.1 BizTalk udvekslingmapper

Ud over konfigurerbare fejlbeskeder findes også stierne til BizTalk udvekslingsmapperne blandt *appSettings* i web.config filen.

```
<appSettings>
  <!-- Stien til den mappe som inputfilerne lægges på efter VSLight metodekaldet SendRequest.
       BizTalk skal sættes til at samle input op fra denne mappe. -->
  <add key="RequestFolderPath" value="\\172.30.58.202\virksomhedssystem\VSLIGHT" />
  <!-- Stien til den mappe som outputfilerne hentes fra efter VSLight metodekaldet GetResponse.
       BizTalk skal sættes til at lægge output i denne mappe. -->
  <add key="ResponseFolderPath" value="\\172.30.58.202\virksomhedssystem2\VSLIGHT" />
```

Det er vigtigt at disse mapper er delt sådan at brugerkontoen for VSLights *application pool* har skriveadgang til dem.

5.2 Dialogservice

I web.config filen findes også angivelsen af adressen på dialogservicens endpoint.

```
<system.serviceModel>

  <client>
    <!-- Dialogservice endpoint som skal justeres efter det miljø der køres på. -->
    <!-- VSLight benytter dialogservicen til at skrive i IOLog og kontrollere abonnementer.  -->
    <endpoint address="http://172.30.58.200/kmd.nemrefusion.Dialog/Service.asmx"
      binding="basicHttpBinding" bindingConfiguration="ServiceSoap"
      contract="DialogService.ServiceSoap" name="ServiceSoap" />
  </client>
```

Dette skal justeres så der peges på den korrekte dialogservice i forhold til det miljø der køres på.

5.3 Abonnenter

Thumbprint for abonnenternes klientcertifikat er registreret i tabellen *VSLightAbonnenter* i databasen. Værdierne for *CvrNummer* og *Beskrivelse* bliver ikke direkte brugt til noget, men bør for en god ordens skyld udfyldes korrekt. Det vigtige er værdien for *KlientcertifikatThumbprint* som kan skrives med store eller små bogstaver og med eller uden mellemrum (47 54 01 5a 50 06 50 87 3c bc b4 d6 bc 6c 60 45 46 bf 6e 8f = 4754015A500650873CBCB4D6BC6C604546BF6E8F).

	CvrNummer	Beskrivelse	KlientcertifikatThumbprint
	19435075	KOMBIT A/S	28 28 ed 18 7c 46 13 55 c7 9f 70 47 e7 74 2e ce 01 28 8b 44
	30808460	DANID A/S	47 54 01 5a 50 06 50 87 3c bc b4 d6 bc 6c 60 45 46 bf 6e 8f
▶*	*NULL*	*NULL*	*NULL*

For at registrere nye abonnenter skal der manuelt indsættes nye rækker i tabellen (via Teknisk Service Desk).