GÆLDS STYRELSEN

Guide til krypteret tilslutning

Indholdsfortegnelse

Baggrundsinformation 3
Flow i produktion 3
Flow i test 5
Centrale Sikkerhedsforanstaltninger ved tilslutning til NyMF 6
Whitelisting 6
Certifikater 6
Tjek af systemleverandør 6
Den Centrale Sikkerhedsløsning (DCS) 6
TastSelv Erhverv 7
Endpoints og snitflader 7
SKAT fordringshavere 8
Fordringshaverportalen 9
Opsætning af kryptering i NyMF 9
Opsætning med SoapUI 10
Opsætning med Java 10
Transport Layer Security 10
WS-policy 11
Kryptering i test 12
IP-whitelisting 12
Bestil IP whitelistet 12
Test: hul igennem til server (browser) 12
Kryptering af forbindelse og requests 13
Hent test VOCES fra NemLog-in 13
Hent NyMF B2B-testcertifikat fra GÆLDSTs hjemmeside 13
Læg certifikater i fordringshaverens system 13
Opsætning af SoapUI 17
Opsætning af Java 21
Test: den krypterede forbindelse (Command Line Interface) 22
Test: kryptering af forbindelse og request (SoapUI) 23

Fordringshaverportalen 24
Bestil testbruger via GÆLDST/UFST 24
Kryptering i produktion 24
IP-whitelistning 24
Bestil IP whitelistet 24
Kryptering af forbindelse og requests 24
Hent VOCES fra MitID 24
Hent NyMF B2B-certifikat fra GÆLDSTs hjemmeside 25
Læg certifikater i fordringshaverens system og opsæt til krypteret tilslutning 25
Registrer VOCES 25
Bestil oprettelse i DCS 25
Opret systembruger i TastSelv Erhverv (registrer VOCES) 25
Opret rolle og tildel rettigheder i TastSelv Erhverv 26
Test: krypteret forbindelse og kryptering af request 26
Fordringshaverportalen 26
Tildel rettigheder i TastSelv Erhverv 26
Test: der kan logges på Fordringshaverportalen 27
Fejlsøgning 27

Baggrundsinformation

Formålet med dette dokument er at guide fordringshavere og systemleverandører til at opnå en sikker tilslutning fra deres system og til Public Sector Revenue Management (PSRM) via Ny Modtag Fordring (NyMF). Her er NyMF den samling af services (interfaces), som man benytter ved en system-til-system tilslutning.

Dokumentet forsøger at give et overblik over, hvordan tilslutningsprocessen ser ud i hhv. test og produktion samt over, hvad fordringshaveren konkret skal gøre for at opnå krypteret tilslutning til NyMF.

Før fordringshaveren kan opnå krypteret tilslutning mod produktion, vil de skulle gennemgå en testfase, som imiterer tilslutningen mod produktion. Testfasen begynder med, at fordringshaveren kontakter Gældsstyrelsen (GÆLDST), som sørger for, at fordringshaveren får:

- tildelt adgang til NyMFs systemdokumentation
- tilsendt og udfyldt testplan
- tildelt testmiljø
- oprettet fordringshaveraftale og filter til testmiljøet

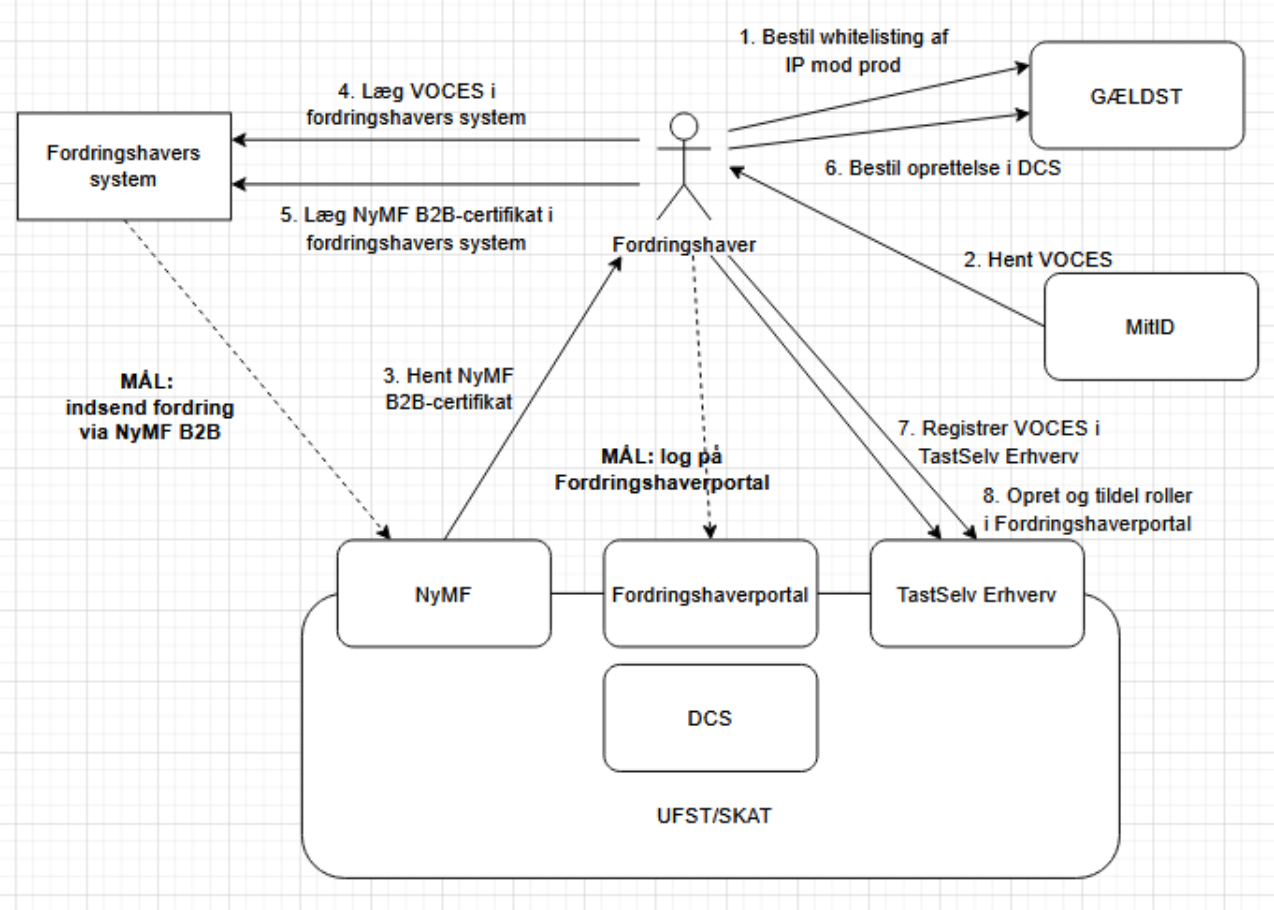
Når disse punkter er på plads, vil dette dokument kunne benyttes som guide for fordringshaveren i deres tilslutning til NyMF. Når tilslutningen er lykkedes, vil fordringshaverens system kunne kommunikere på sikker vis med NyMF – og fx indberette fordringer, samt hente kvitteringer og underretninger.

OBS! Opsætningen af den krypterede tilslutning er en tidskrævende og vanskelig proces at fejlsøge! Erfaring gennem flere år viser, at virksomheder ofte undervurderer, hvor lang tid dette tager – på papiret ser det forholdsvist enkelt ud. Sørg derfor for at afsætte ekstra tid til den krypterede forbindelse, både mod test og produktion.

Flow i produktion

Når en fordringshaver går i produktion, vil følgende overordnede trin skulle gennemføres for at opnå fuld krypteret tilslutning fra fordringshaverens system til NyMF

- Whitelisting af IP-adresser til produktion (punkt 1)
- Kryptering af forbindelse og requests (punkt 2-5)
- Registrering af certifikat i TastSelv Erhverv (punkt 6-7)
- Evt.: adgang til Fordringshaverportalen (punkt 8)



Jf punkt 1: fordringshaveren skal anmode GÆLDST om at få whitelistet de relevante IP-adresser for dermed at få åbnet firewallen mod produktion.

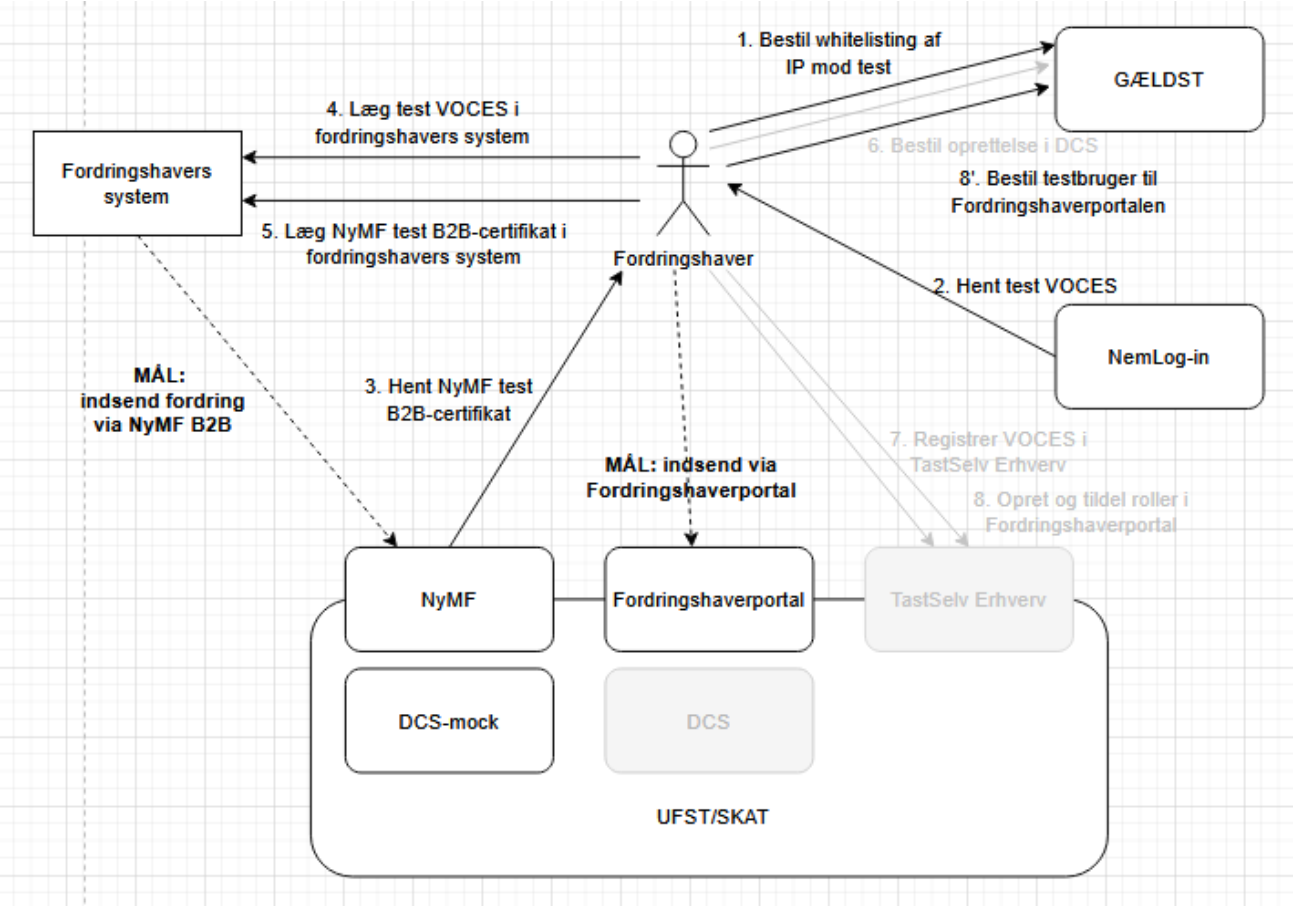
Jf. punkt 2-5: fordringshaveren skal bestille eget virksomhedscertifikat fra MitID Erhverv samt hente produktionscertifikat fra GÆLDSTs hjemmeside. Disse certifikater skal lægges i fordringshaverens system, og bruges i forbindelse med opsætning af krypteret forbindelse og kryptering af requests.

Jf. punkt 6-7: fordringshaveren skal anmode GÆLDST om at blive oprettet i Den Centrale Sikkerhedsløsning (DCS). Derudover skal fordringshaveren selv sørge for at logge på SKAT TastSelv Erhverv og her registrere deres virksomhedscertifikat samt tildele det en ”systembrugerrolle”.

Jf punkt 8: i TastSelv Erhverv skal fordringshaveren tildele relevante medarbejdere rollerne ”Administrere fordringer” og ”Se fordringer” i Fordringshaverportalen. OBS! dette trin er kun relevant for hybrid- og portalbrugere.

Flow i test

Når en fordringshaver skal teste den krypterede tilslutning mellem fordringshaversystemet og NyMF, vil stort set samme flow som i produktion skulle følges. Der er dog undtagelser, som kort gennemgås her.



Jf. punkt 1: fordringshaveren skal anmode GÆLDST om at få whitelistet de relevante IP-adresser, for dermed at få åbnet firewallen mod testmiljøet. Fordringshaveren får tildelt et testmiljø i forbindelse med deres onboarding-proces.

Jf. punkt 2-5: fordringshaveren skal bestille eget test-virksomhedscertifikat fra NemLog-in samt hente testcertifikatet fra GÆLDSTs hjemmeside. Ligesom i produktion, skal disse certifikater lægges i fordringshaverens system og bruges i forbindelse med opsætning af den krypterede forbindelse og kryptering af requests.

Jf. punkt 6-8: disse punkter er ikke en del af testfasen. Altså skal fordringshaveren hverken benytte DCS eller TastSelv Erhverv, så længe testfasen pågår.

Jf. punkt 8': fordringshaveren skal anmode GÆLDST om at få oprettet en testbruger i Fordringshaverportalen. Når fordringshaveren skal teste login til Fordringshaverportalen, vil de blive mødt af en drop-down-menu frem for en MitID-login-side. Her vil fordringshaveren kunne finde sig selv i bunden af drop-down-menuen. OBS! dette trin er kun relevant for hybrid- og portalbrugere.

Centrale Sikkerhedsforanstaltninger ved tilslutning til NyMF

Whitelisting
For at lukke trafik fra fordringshaveren igennem NyMFs firewalls, skal fordringshaveren kontakte UFST og bede om at få deres IP-adresser whitelistet. I testfasen skal fordringshaveren bede om at blive whitelistet til nonprod, og når fordringshaveren går i produktion, skal de bede om at få deres adresser whitelistet til produktion.

Certifikater
For at kryptere både forbindelse og requests skal fordringshaveren være i besiddelse af et server- og et klient-certifikat. Fordringshaveren skal downloade server-certifikatet (NyMF-certifikat) og tilføje dette til deres truststore, og de skal bestille et virksomheds-klient-certifikat af typen VOCES-3 (virksomhedscertifikat af typen: Offentlige Certifikater til Elektronisk Service).

Fordringshaverens VOCES-certifikat bruges til disse 3:

1. Kryptering af system-til-system forbindelsen.
2. Kryptering af beskeden.
3. Dekryptering af indkommende beskeder.

I punkt 3 bruges VOCES certifikatet via fordringshaverens truststore (som indeholder NyMF-certifikatet) til at dekryptere indkommende beskeder.

Denne noget utraditionelle tilgang til certifikater benytter NyMF til at opnå fuldt krypteret, sikker udveksling af information mellem fordringshaverens system og NyMF.

Tjek af systemleverandør
I NyMF er der implementeret et tjek, som sikrer, at en given systemleverandør har tilladelse til at sende ind på vegne af en fordringshaver. Dette tjek undersøger, om det fordringshaverid og systemindberetterid, som indgår i et request, stemmer overens med de id'er, som er registreret i fordringshaveraftalen i PSRM.

Den Centrale Sikkerhedsløsning (DCS)
For at kunne sende requests ind mod NyMF i produktion skal en fordringshaver og/eller systemleverandør være registreret i Den Centrale Sikkerhedsløsning (DCS). Det samme gælder for at kunne logge ind i Fordringshaverportalen. De oplysninger, som fordringshaverens eller systemleverandørens certifikat indeholder, tjekkes op imod det CVR, som er registreret i DCS. Hvis disse data ikke stemmer overens, vil fordringshaveren ikke opnå forbindelse til NyMF.

OBS! For at kunne foretage handlinger i Fordringshaverportalen vil man desuden skulle knytte bestemte rettigheder til det relevante CVR/certifikat.

OBS! Interne SKAT fordringshavere skal ikke oprettes i DCS, men skal have oprettet en rolle via Omada.

Rettigheder i DCS

Når fordringshaveren eller systemleverandøren bliver oprettet i DCS, knyttes de som regel til bestemte rettigheder – oftest rettighederne: Læser og Sagsbehandler. Dette sikrer, at fordringshaveren eller systemleverandøren kan udføre de nødvendige handlinger i PSRM.

DCS i test og produktion

Mens fordringshaveren tester tilslutningen til NyMF, benytter de et tildelt testmiljø fremfor at tilgå produktion. De testmiljøer, som stilles til rådighed for fordringshaverne, er – modsat produktion – ikke forbundet med DCS, og derfor foregår fordringshaverens testfase uden om denne sikkerhedsløsning. Om end det ikke er ideelt, at testfasen således adskiller sig fra gangen i produktion, så har den historiske udvikling i NyMF betydet, at dette er status pt.

TastSelv Erhverv

Når fordringshaveren skal tilgå PSRM via NyMF kontrolleres det, at deres informationer findes hos SKAT TastSelv, og at de har de korrekte rettigheder. Derfor skal der i SKAT TastSelv eksistere en Systembrugerrolle med de samme informationer, som certifikatet indeholder (en systembruger er lig med et virksomhedscertifikat).

Derfor skal fordringshaveren efter oprettelse i DCS, registrere deres certifikat i SKAT TastSelv Erhverv. I den forbindelse skal der oprettes en systembrugerrolle med de samme informationer – CVR og UID – som indgår i certifikatet. Denne systembruger kan så tilføje de rettigheder, som skal bruges i PSRM. Hvis relevant, kan systembrugeren også tildele rettighederne til de relevante medarbejdere.

Endpoints og snitflader

For alle fordringshavere, der ikke hører under SKAT, benyttes NyMF HTTPS med Mutual Authentication. På testmiljøerne (sit-miljøerne) benyttes port **6443** til at sikre Mutual Authentication.

Eksterne fordringshavere kan bruge følgende endpoints til at forbinde til rette **testmiljø**, snitflade-version af NyMF, port, samt service (her erstattes XX af det miljø man får tildelt):

- https://nymf-b2b-soap-oio-secure-sitXX.inddr.dk:6443/latest/services/FordringIndberetService?wsdl
- https://nymf-b2b-soap-oio-secure-sitXX.inddr.dk:6443/latest/services/KvitteringHentService?wsdl
- https://nymf-b2b-soap-oio-secure-sitXX.inddr.dk:6443/latest/services/UderretSamlingHentService?wsdl

Endpoints mod produktion kan fordringshaveren finde i den dokumentation, som de har fået tilsendt i forbindelse med onboarding-processen.

I alle tilfælde anbefales det, at fordringshaveren vælger seneste snitflade-version, idet denne vil indeholde de seneste ændringer og tilføjelser til hver af de eksisterende services. Det sker automatisk når man beholder teksten ”latest”. Det kan imidlertid erstattes af fx v6.5.0, men en gammel snitflade vil mangle funktionalitet, som eksempel kan nævnes at v6.13.0, har årsagskoderne FORM og REPL. De er ikke en del af underretningsamlinghent-servicen, hvis fordringshaveren vælger en tidligere version af snitfladen. I tillæg vil de ældste snitflader efterhånden udfases og man vil være tvunget til at skifte til en nyere version. Nye snitflader, som automatisk følger med ”latest”, vil som hovedregel altid være bagudkompatible.

SKAT fordringshavere

Størstedelen af fordringshavere er eksterne, og disse forbinder til NyMF over OIO-snitfladen på en internetforbindelse. Nogle fordringshavere er SKAT selv, og disse såkaldte ”interne fordringshavere” forbinder på anden måde. Listen af interne fordringshavere pr. 2026 er følgende:

- STI (Sap38 til inddrivelse)
- KOBRA
- DMO (Skattekontoen)
- ELO

Disse fordringshavere forbinder til NyMF over SKAT leverandørnet (også kaldet MPLS). Alle på nær DMO benytter separat snitflade (WSDL/XSD), kaldet SKAT-XML. DMO benytter OIO. SKAT-XML kører på anden port end OIO, og porten i produktion samt adressen for SIT er derfor anderledes.

I test bruges følgende sit-adresser for SKAT:

- https://nymf-b2b-soap-skat-secure-sitXX.inddr.dk:6443/V6.13.0/services/FordringIndberetService?wsdl
- https://nymf-b2b-soap-skat-secure-sitXX.inddr.dk:6443/V6.13.0/services/KvitteringHentService?wsdl
- https://nymf-b2b-soap-skat-secure-sitXX.inddr.dk:6443/V6.13.0/services/UderretSamlingHentService?wsdl

Bemærk, at sit-adressen skal oversættes til korrekt IP; man kan ikke benytte internet-DNS til at oversætte IP til en Leverandørnet-vendt adresse. IP på Leverandørnettet findes i den dokumentation, fordringshaveren har fået tilsendt i forbindelse med onboardingprocessen. Så vidt muligt skal fordringshaver sætte hostnavn-oversættelse op i egen DNS, eller i host-fil på server.

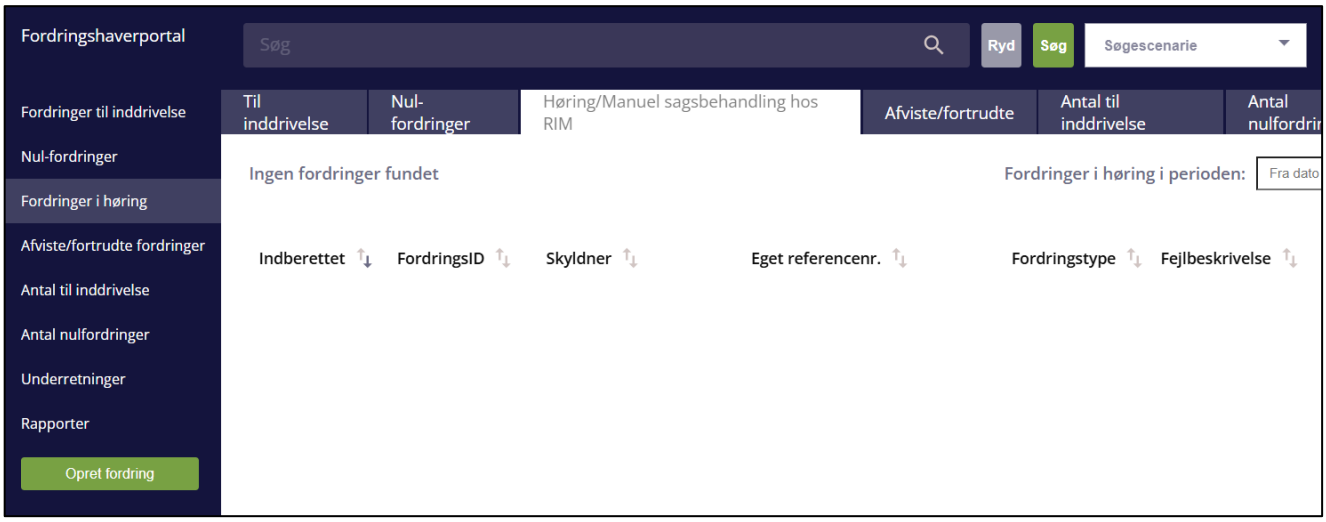
Endpoints mod produktion kan fordringshaveren finde i den dokumentation, som de har fået tilsendt i forbindelse med onboarding-processen.

Åbning til SKAT interface over Leverandørnettet skal ske således:

1. Fordringshaver foretager åbning ud mod leverandørnettet med korrekt sit / prod IP og port
2. Fordringshaver tester netværkshul
3. Fordringshaver sætter HTTPS Mutual Auth-kryptering op

Interne fordringshavere skal være opmærksomme på, at SKAT-snitfladen i NyMF ikke benytter WS-policy, men i stedet benytter basic-auth. I den forbindelse skal interne fordringshavere kontakte Team Onboarding, som vil bestille tilføjelse af en ny bruger i brugerstyringen for SKATs snitflade hos NyMF og Komponenter. Dette skal gøres én gang i test, og igen når fordringshaveren går i produktion.

Fordringshaverportalen



Når fordringshaveren er blevet oprettet i DCS, har registreret deres certifikat i SKAT TastSelv Erhverv, samt har fået oprettet en fordringshaveraftale i PSRM, vil de kunne tilgå Fordringshaverportalen:

1. Oprettet i DCS
2. Registreret i SKAT TastSelv Erhverv
3. Fordringshaveraftale i PSRM

Dette forudsætter dog, at 3) fordringshaveraftale i PSRM er oprettet som portal- eller hybridbruger. En fordringshaver, som alene har en system-til-system-løsning, vil ikke kunne oprette og korrigere fordringer gennem Fordringshaverportalen. Dog skal systembrugere benytte fordringshaverportalen til at besvare høringsfordringer og hente rapporter.

Kort opsummeret er fordringshaverportalen en hjemmeside, der udgør et brugervenligt alternativ eller supplement til fordringshaverens system-til-system-løsning. På fordringshaverportalen kan fordringshaveren bl.a. hente lister af fordringer til inddrivelse, nul-fordringer, fordringer i høring og afviste/fortrudte fordringer. Derudover har fordringshaveren mulighed for at hente underretning samt at fremsøge specifikke fordringer på forskellige id-numre. De konkrete handlinger, som en bruger har adgang til i fordringshaverportalen, afhænger af brugerens rettigheder. En bruger med læserettigheder kan godt hente underretninger, men kan eksempelvis ikke indberette fordringer.

Opsætning af kryptering i NyMF

Når fordringshaveren skal indsende requests fra fordringshaversystemet mod NyMF, kræver det en opsætning af den krypterede forbindelse mellem systemerne, samt en kryptering af det request, der skal sendes. I dette dokument præsenterer vi to mulige eksempler på, hvordan en sådan opsætning kan se ud. Det ene eksempel viser, hvordan certifikater kan opsættes til kryptering af forbindelse og besked i SoapUI, og det andet viser, hvordan dette kan gøres i Java. Begge dele er dog primært ment som inspiration og er altså ikke direkte anvendelige, plug-and-play-løsninger.

Opsætning med SoapUI
SoapUI er et redskab, der kan bruges til at generere requests vha. fx wsdl-filer. I denne kontekst vil wsdl-filen beskrive NyMFs servicegrænseflade, og ved at importere en wsdl-fil i SoapUI kan fordringshaveren oprette og afvikle tests uden selv at skulle opbygge request-xml-strukturen fra bunden.

Hvis fordringshaveren ønsker, at den krypterede tilslutning mellem fordringshaversystemet og NyMF skal gå via SoapUI, skal dette opsættes til at overholde NyMFs sikkerhedsstandarder. Når det er gjort, vil fordringshaveren kunne indsende requests via SoapUI på sikker vis.

Via SoapUI kan fordringshaveren benytte de 3 NyMF-services: indberet fordring, hent kvittering og hent underretning. Derudover vil fordringshaveren kunne vælge hvilken snitfladeversion af NyMF, de ønsker at benytte (seneste version anbefales), og de vil kunne modtage den wsdl-fil, som svarer til den valgte service og snitflade. Dette gøres ved at tilpasse de endpoints, som er nævnt i kapitlet Endpoints, til det testmiljø, fordringshaveren har fået tildelt, til den ønskede snitfladeversion, samt til den ønskede service. Dermed kan fordringshaveren hente den korrekte struktur for de xml-filer, som bruges til at kommunikere med NyMF.

Opsætning med Java
Hvis fordringshaveren ønsker, at den krypterede tilslutning mellem fordringshaversystemet og NyMF skal ske i Java, kan kodeeksempel i kapitlet Opsætning af Java benyttes som inspiration. Dette projekt indeholder bl.a. wsdl- og xsd-filer, som beskriver funktionaliteten og datastrukturerne af de services, som NyMF tilbyder. Ligesom i SoapUI vil fordringshaveren også her kunne bruge relevante endpoints til at målrette deres kommunikation mod det ønskede testmiljø, snitfladeversion og service.

Yderligere indeholder projektet bl.a. NyMFs WS-policy, samt et eksempel på en klient keystore, hvilket fordringshaveren kan benytte som inspiration, hvis de ønsker at sikre den krypterede tilslutning mellem fordringshaversystemet og NyMF i Java.

Transport Layer Security
For at sikre, at kommunikationen mellem fordringshaversystemet og NyMF foregår efter sikre, fuldt krypterede kanaler, benyttes HTTP over TLS. NyMF benytter i dag TLS version 1.3 og tillader på nuværende tidspunkt ikke SSLv2Hello, SSLv3, TLSv1, TLSv1.1 eller RC4. Fordringshaveren bør derfor anvende TLS v1.3, når forbindelsen mellem de 2 systemer skal krypteres.

Bemærk, at NyMF desuden er konfigureret til at afvise forbindelser, der anvender følgende ciphers, og derfor bør fordringshaveren undgå at benytte disse.

- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

WS-policy

Når fordringshaveren skal indsende requests mod NyMF, skal de sørge for, at den krypteringsstandard, som NyMF anbefaler, overholdes. NyMF anvender den Web Service Policy, som kan ses nedenfor og som anbefaler, at requestet både krypteres og signeres. Dette skal sikre, at kun den tiltænkte modtager kan læse indholdet, samt at indholdet er uændret og afsenderen er kendt. Kort opsummeret anbefaler WS-standarden, at Basic256Sha256 sikkerhedsprofilen følges, og fordringshaveren opfordres til at:

- Indsætte tidsstempel
- Signere requestet ved brug af fordringshaverens VOCES
    - Benytte signatur-algoritmen til signering af digest'et
      http://www.w3.org/2000/09/xmldsig#rsa-sha1
    - Benytte signatur-kanonisering til at sikre ensartning af requestet
      http://www.w3.org/2001/10/xml-exc-c14n#
    - Benytte "digest" til at hashe det kanoniserede request
      http://www.w3.org/2000/09/xmldsig#sha1
    - Både body og tidsstempel signeres
- Kryptere requestet ved at anvende NyMF-certifikatet
    - Benytte symmetrisk algoritme til at kryptere og dekryptere requestet med
      http://www.w3.org/2001/04/xmlenc#aes256-cbc
    - Benytte nøglekrypteringsalgoritmen til at sikre den symmetriske algoritme
      http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p
    - Kun body krypteres

Selve WS-standarden kan ses her:

```
<?xml version="1.0" encoding="UTF-8"?>
  <wsp:Policy
  xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
  xmlns:wsp="http://www.w3.org/ns/ws-policy"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  wsu:Id="skat-b2b-x509-policy">
  <wsp:ExactlyOne>
   <wsp:All>
    <sp:AsymmetricBinding>
     <wsp:Policy>
      <sp:InitiatorToken>
       <wsp:Policy>
        <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/AlwaysToRecipient">
         <wsp:Policy>
          <sp:WssX509V3Token10/>
         </wsp:Policy>
        </sp:X509Token>
       </wsp:Policy>
      </sp:InitiatorToken>
      <sp:RecipientToken>
       <wsp:Policy>
        <sp:X509Token sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702/IncludeToken/Never">
         <wsp:Policy>
```

```
            <sp:RequireThumbprintReference />
            <sp:WssX509V3Token10/>
          </wsp:Policy>
        </sp:X509Token>
      </wsp:Policy>
    </sp:RecipientToken>
    <sp:AlgorithmSuite>
      <wsp:Policy>
        <sp:Basic256Sha256/>
      </wsp:Policy>
    </sp:AlgorithmSuite>
    <sp:Layout>
      <wsp:Policy>
        <sp:Lax/>
      </wsp:Policy>
    </sp:Layout>
    <sp:IncludeTimestamp/>
    <sp:OnlySignEntireHeadersAndBody/>
    <sp:SignBeforeEncrypting/>
  </wsp:Policy>
</sp:AsymmetricBinding>
<sp:SignedParts>
  <sp:Body/>
</sp:SignedParts>
<sp:EncryptedParts>
  <sp:Body/>
</sp:EncryptedParts>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
```

Kryptering i test

IP-whitelisting

Bestil IP whitelistet

Fordringshaveren får tildelt et testmiljø, når onboarding-processen påbegyndes. Fordringshaveren skal anmode GÆLDST om at få de IP-adresser, som de bruger i test, whitelistet således, at firewallen bliver åbnet for de relevante IP-adresser mod det tildelte testmiljø. Dette er nødvendigt, hvis fordringshaveren skal kunne sende requests ind til deres testmiljø.

Test: hul igennem til server (browser)

Når fordringshaveren har fået whitelistet de relevante IP-adresser, kan de teste, om der er hul igennem til serveren *uden om* den krypterede forbindelse. Dette gøres ved at forbinde til NyMF-integrationskomponenten frem for NyMF-b2b. Denne test kan være relevant i starten af testfasen, hvor certifikaterne endnu ikke er opsat, og man bare ønsker at se, om firewallen er blevet åbnet.

Fordringshaveren kan her forsøge at indtaste følgende endpoints i en browser (hvor XX erstattes af det nummer testmiljø man har fået tildelt):

- https://nymf-integration-soap-oio-sitXX.inddr.dk/V6.13.0/services/KvitteringHentService?wsdl
- https://nymf-integration-soap-oio-sitXX.inddr.dk/V6.13.0/services/FordringIndberetService?wsdl
- https://nymf-integration-soap-oio-sitXX.inddr.dk/V6.13.0/services/UnderretSamlingHentService?wsdl

Hvis firewallen er åbnet succesfuldt, vil fordringshaveren se den relevante wsdl-fil i browseren.

Kryptering af forbindelse og requests

Hent test VOCES fra NemLog-in
For at teste den krypterede tilslutning til NyMF samt kryptering af de requests, der sendes fra fordringshaversystemet til NyMF, skal fordringshaveren indledningsvist hente et klient test-certifikat:

1. Gå til siden https://testportal.test-devtest4-nemlog-in.dk/BO
2. Opret test brugerorganisation og gem oplysningerne
3. Opret certifikatprofil
4. Bestil certifikat
5. Udsted certifikat
6. Download certifikat

Hent NyMF B2B-testcertifikat fra GÆLDSTs hjemmeside
Dernæst skal fordringshaveren hente NyMF server-certifikatet. For at hente NyMFs gældende test-certifikat gøres følgende:

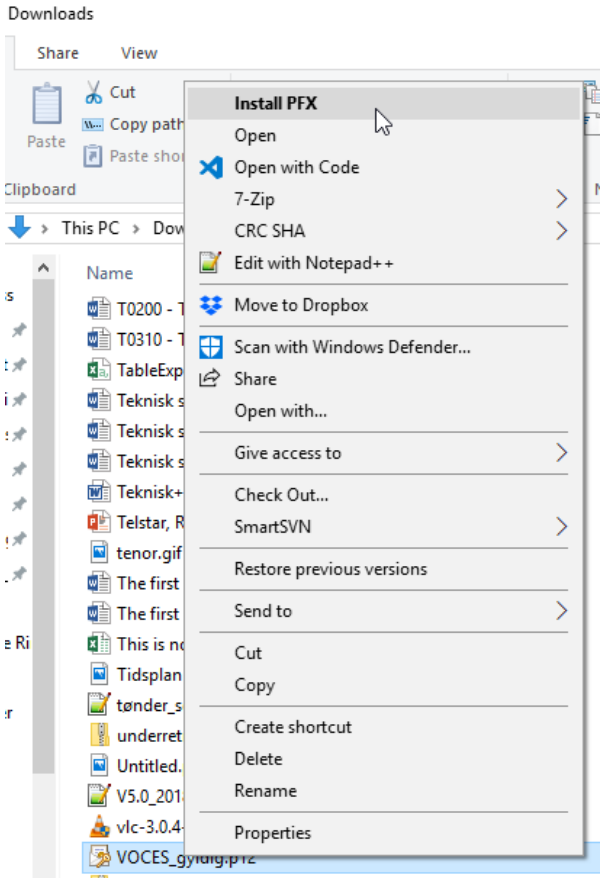
1. Gå til siden: https://gaeldst.dk/fordringshaver/find-vejledning/teknisk-tilslutning-og-adgang/krypteret-tilslutning
2. Find testcertifikatet nederst på siden, download dette

Læg certifikater i fordringshaverens system
Fordringshaveren skal sørge for, at NyMF test-certifikatet lægges i den truststore, som fordringshaversystemet opererer med, samt at deres eget test-VOCES lægges i fordringshaversystemet.

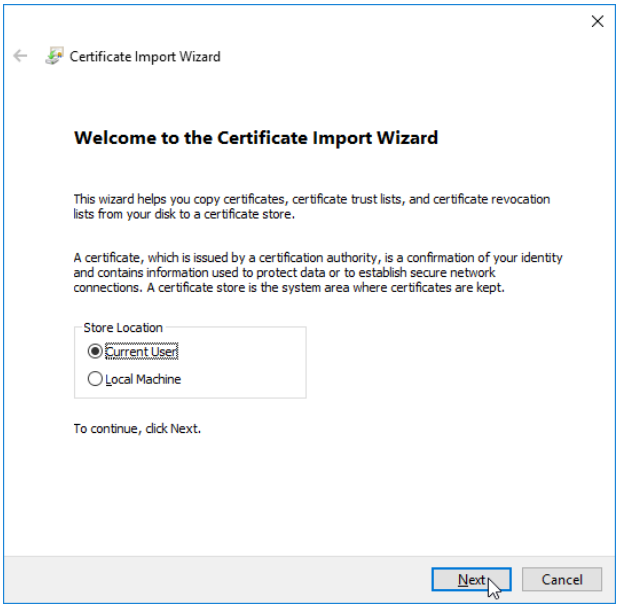
Klient-certifikatet kan installeres ved at følge disse punkter:

1. Download certifikatet

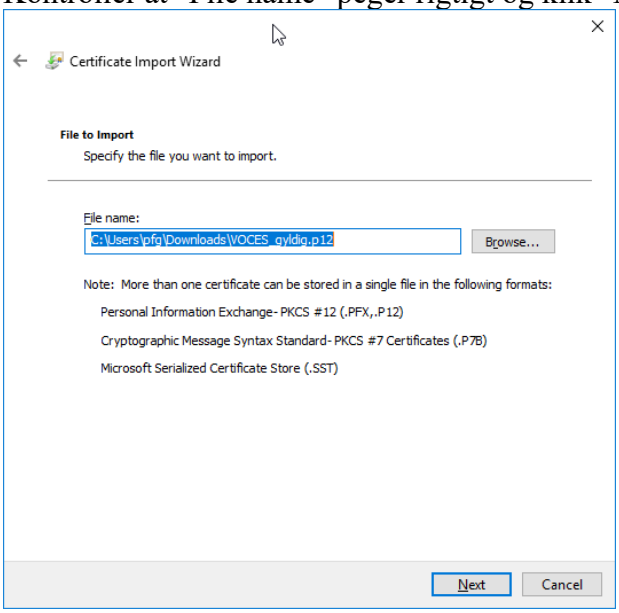
2. Find certifikatet og dobbeltklik på det eller højreklik og vælg "Install PFX"



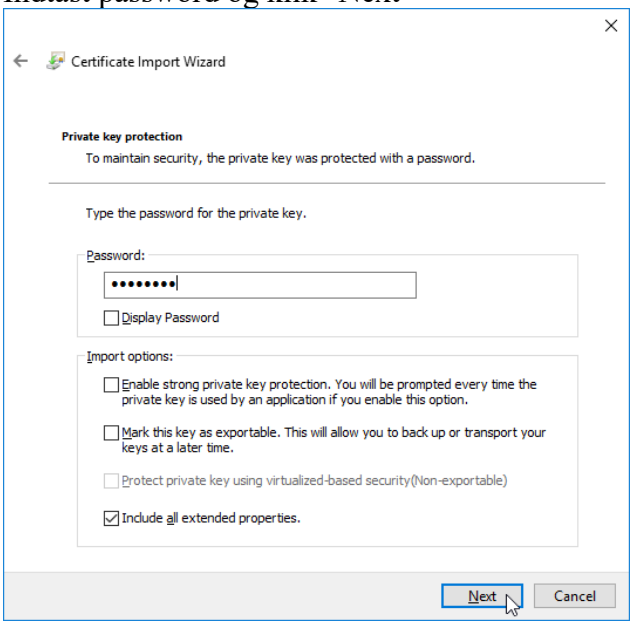
3. Klik "Next"



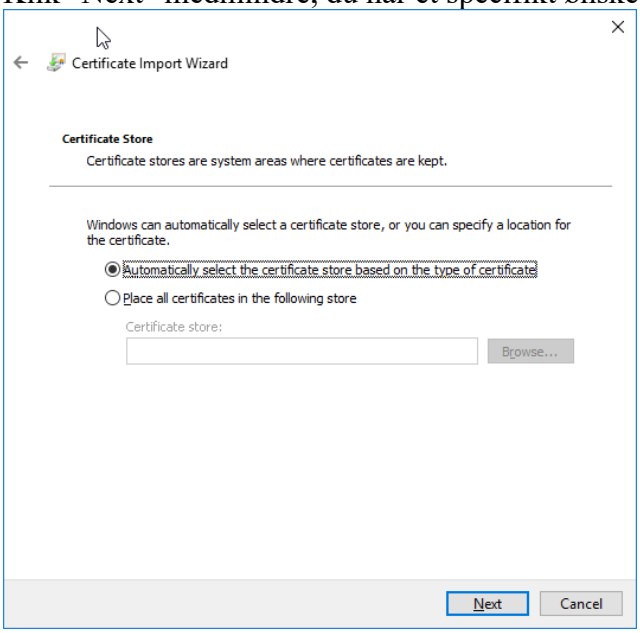
4. Kontroller at "File name" peger rigtigt og klik "Next"



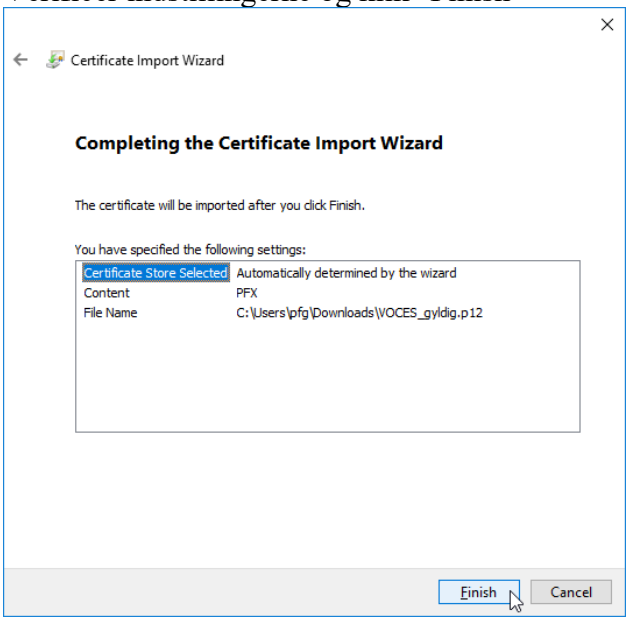
5. Indtast password og klik "Next"



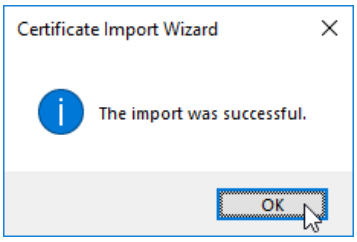
6. Klik "Next" medmindre, du har et specifikt ønske, om hvor certifikatet skal placeres



7. Verificer indstillingerne og klik "Finish"



8. Certifikatet skulle nu være installeret



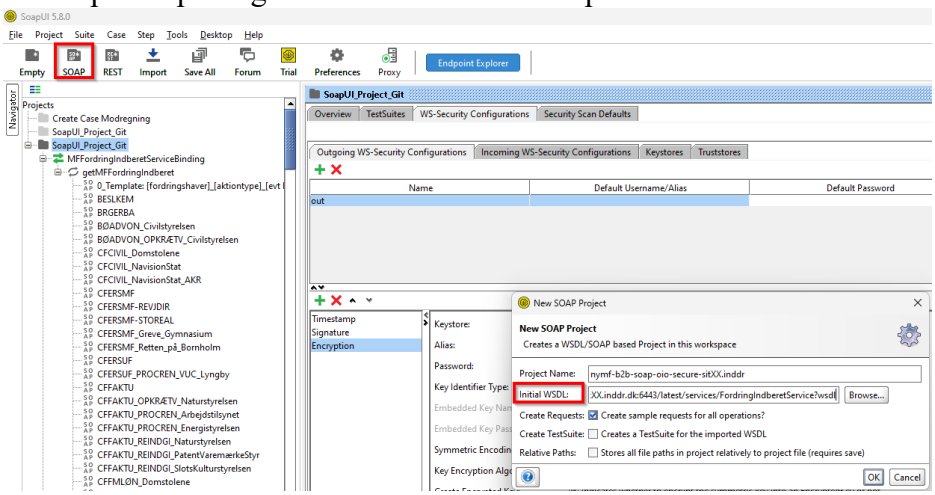
Opsætning af SoapUI

Opsætning af projekt i SoapUI

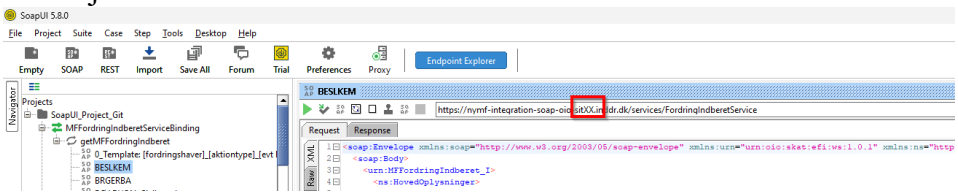
Hvis man som fordringshaver ønsker at gøre brug af SoapUI til at forbinde med NyMF, kan man opsætte et projekt ved at følge disse trin

1.Åben SoapUI

2.Klik på SoapUI og indsæt det relevante endpoint med det relevante test-miljø:



3.Åben requestet, og husk at omdøbe IP-adressen således, at den er rettet mod det relevante testmiljø:



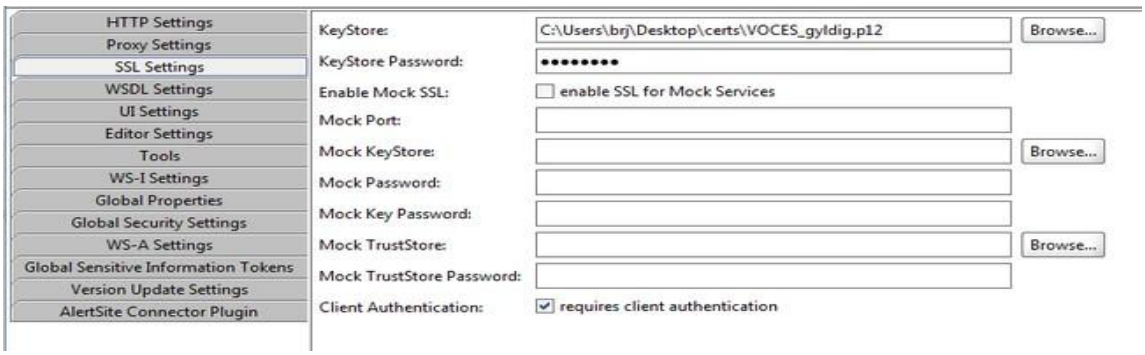
Kryptering af forbindelsen – opsætning af SoapUI til TLS

For at sikre, at kommunikationen mellem klient og server foregår ad fuldt krypterede kanaler, benyttes HTTP over TLS. Fordringshaveren bedes om at konfigurere SoapUI til TLS v1.3, som på nuværende tidspunkt er nyeste version, som NyMF er konfigureret til.

Først opsættes selve VOCES i SoapUI:

1. Åben SoapUI
2. Gå til Files/Preferences
3. Under SSL udfyldes
    a. Stien til hvor fordringshaveren har lagt VOCES-testcertifikat

b. Password



Dernæst konfigureres SoapUI til TLS v1.3:

1. Åbn folderen C:\Program Files\SmartBear\SoapUI-5.2.1\bin (den kan muligvis også gemme sig her, hvis man ikke kan finde den: C:\Program Files (x86)\SmartBear\SoapUI-5.2.1\bin)
2. Åbn filen SoapUI-5.2.1.vmoptions med fx Notepad
3. Tilføj linjen "-Dsoapui.https.protocols=TLSv1.3"
4. Genstart SoapUI

Kryptering af beskeden – opsætning af SoapUI til WSS

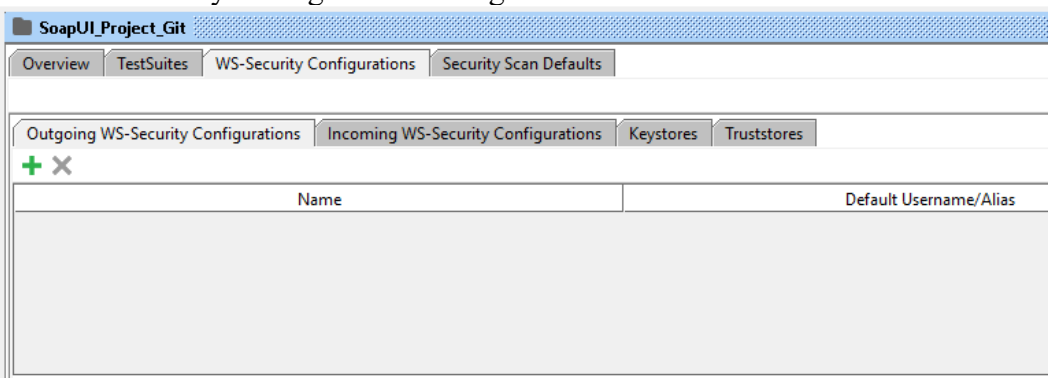
På nuværende tidspunkt bør fordringshaveren have oprettet krypteret forbindelse, og dermed kunne kommunikere med NyMF-serveren.

Ved indsendelse af et request, vil fordringshaveren dog få en fejlmeddelelse i stil med *A security error was encountered when verifying the message*. Denne besked fås, fordi requestet endnu ikke er krypteret. For at kryptere de requests, der sendes mod NyMF, skal SoapUI opsættes til at anvende den WS-politik, som NyMF kræver, og som er præsenteret i kapitel WS-policy.

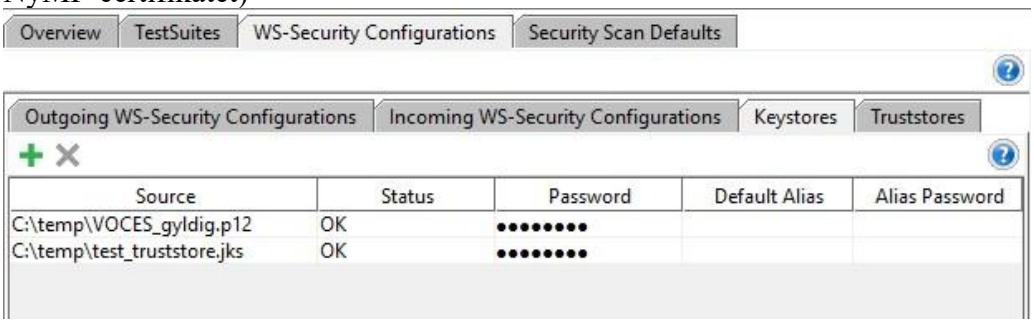
For at sørge for at de requests, der sendes fra fordringshaversystemet til NyMF følger denne standard skal fordringshaveren bruge deres test-VOCES, samt test NyMF-certifikatet.

Tilføj certifikaterne

1. Dobbeltklik på SoapUI-projekt/folder
2. Åbn WS-Security Configuration-dialogen

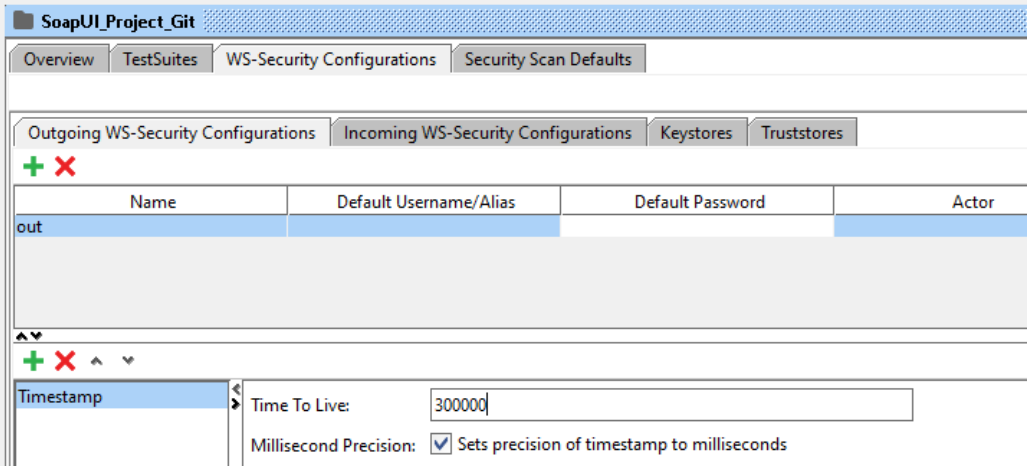


3. Gå til Keystores, og importer VOCES test-certifikatet og jeres truststore (som indeholder NyMF-certifikatet)

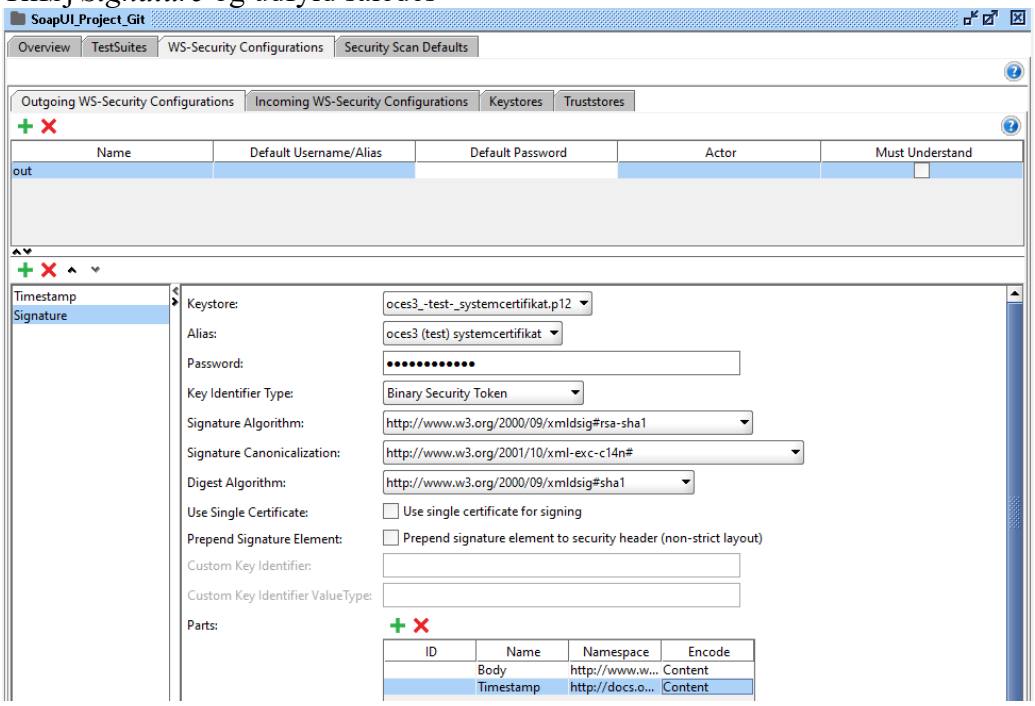


Opsæt udgående trafik – timestamp, signatur og kryptering – ifl. NyMFs WS-policy

4. Under *Outgoing WS-Security Configuration* tilføjes *Timestamp*



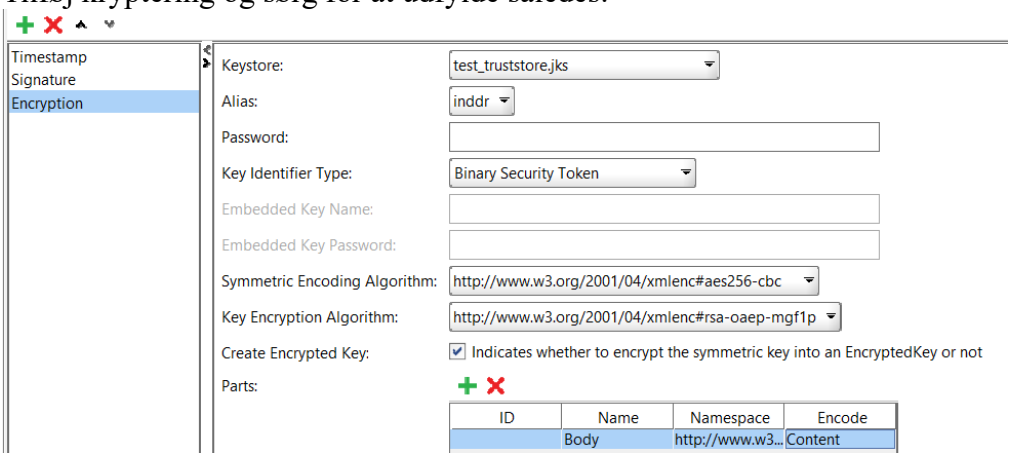
5. Tilføj *Signature* og udfyld således



   a. Under *Key Identifier Type* vælges *Binary Security Token*

b. Under *Signature Algorithm* vælges
http://www.w3.org/2000/09/xmldsig#rsa-sha1
c. Under *Signature Canonicalization* vælges
http://www.w3.org/2001/10/xml-exc-c14n#
d. Under *Digest Algorithm* vælges
http://www.w3.org/2000/09/xmldsig#sha1
e. Under *Parts* udvælges de dele af det udgående request, der skal krypteres
   i. Name: Body
   Namespace: http://www.w3.org/2003/05/soap-envelope
   Encode: Content
   ii. Name: Timestamp
   Namespace: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
   Encode: Content

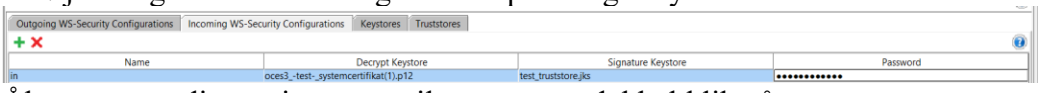
6. Tilføj kryptering og sørg for at udfylde således:



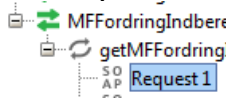
a. Under *Key Identifyer Type* vælges *Binary Security Token*
b. Under *Symmetric Encoding Algorithm* vælges
http://www.w3.org/2001/04/xmlenc#aes256-cbc
c. Under *Key Encryption Algorithm* vælges
http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p
d. Under *Parts* tilføjes *Body*, som er den del af requestet, der skal signeres
   i. Name: Body
   Namespace: http://www.w3.org/2003/05/soap-envelope
   Encode: Content

Opsæt indgående trafik

7. Tilføj konfigurationer for indgående requests og udfyld således:

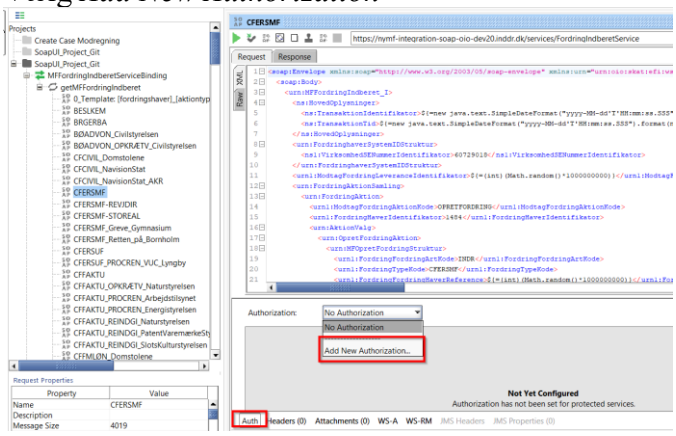


8. Åbn request-editoren i menuen til venstre, og dobbeltklik på et request



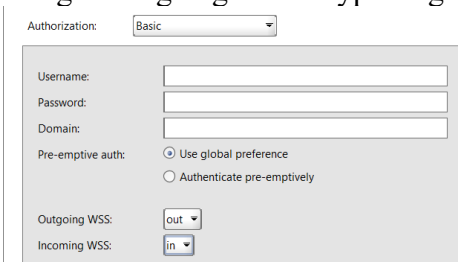
9. Tilføj kryptering og dekryptering til beskeder

a. Vælg *Add New Authorization*



b. Vælg *Basic*

c. Vælg ind- og udgående kryptering



Opsætning af Java

Hvis man som fordringshaver ønsker at tilslutte sig NyMF vha. Java, kan det Java-projekt, som indgår i denne dokumentpakke, bruges som inspiration. Bemærk, at Apache Maven er påkrævet for at køre klienten, og min. Java 8 skal bruges til at bygge projektet.

Fordringshaveren kan bruge projektet som inspiration til, hvordan requests og interface skal struktureres, samt til hvordan klient-keystore kan se ud. Vær opmærksom på, at projektet kun er ment som inspiration for fordringshaverens implementering; bl.a. snitflade, testmiljø og certifikater mm. skal opdateres, for at projektet bliver funktionelt for fordringshaveren.

Projektet indeholder en test (MFKvitteringHentTest), der tester tilslutningen til et givent testmiljø gennem et kald til KvitteringHent-servicen. Denne kan fordringshaveren med fordel også benytte sig af, når den krypterede tilslutning til NyMF testes.

Testen kan afvikles således:

1. Pak filen ud
2. Gå til roden af mappen skat-ici-b2b-sample-client
3. Kør kommandoen "mvn clean verify"
4. Det forventes at tage omkring 1 minut, hvorefter resultaterne af testen vises. Her skulle der gerne stå, at 1 test var kørt uden fejl.
5. Som default forventes det, at der returneres en response med fejlkode 400 ("Systemleverandør der indberetter, kan ikke indberette for den angivne fordringshaver").

Dette skyldes, at det vedlagte certifikat ikke er tilknyttet en egentlig fordringshaver. Responsen viser dog stadig, at tilslutningen til miljøet er succesfuldt.

6. For at fordringshaveren skal kunne teste sine fordringer, skal fordringshaverens certifikat tilføjes til src\test\resources\clientKeystore.jks med alias client, password til keystore er "password". Husk også at opdatere SE Nummer og FordringshaverID i MFKvitteringHentTest.java

Tip: Slå full debugging til / kør programmet med -Djavax.net.debug=all

Test: den krypterede forbindelse (Command Line Interface)
Hvis fordringshaveren ønsker at verificere, at der er hul igennem til testmiljøet, og at der kan hentes certifikat, skal dette ske fra den maskine, der opretter forbindelse til NyMF. Mulige test-værktøjer afhænger af den anvendte maskines opsætning, samt hvilke rettigheder den benyttede bruger har adgang til. Her gennemgås tests med Windows, Linux og browser.

Windows server
- cmd med telnet
  - Indtast følgende i terminalen: telnet nymf-b2b-soap-oio-secure-sit09.inddr.dk 6443
  - Ved succesfuld forbindelse fås outputtet:
    - Trying 5.44.139.48...
    - Connected to nymf-b2b-soap-oio-secure-sit09.inddr.dk
- Powershell
  - Indtast følgende i terminalen:
    Test-NetConnection -ComputerName nymf-b2b-soap-oio-secure-sit09.inddr.dk -Port 6443
  - Ved succesfuld forbindelse fås outputtet:
    - ComputerName : nymf-b2b-soap-oio-secure-sit09.inddr.dk
    - RemoteAddress : 5.44.139.48
    - RemotePort : 6443
    - InterfaceAlias : Ethernet 23
    - SourceAddress : X.X.X.X
    - TcpTestSucceeded : True

Linux server
- cmd med telnet
  - Indtast følgende i terminalen: telnet nymf-b2b-soap-oio-secure-sit09.inddr.dk 6443
  - Ved succesfuld forbindelse fås outputtet:
    Trying 5.44.139.48...
    - Connected to nymf-b2b-soap-oio-secure-sit09.inddr.dk
- OpenSSL
  - Indtast følgende i terminalen:
    openssl s_client -connect nymf-b2b-soap-oio-sit09-secure.inddr.dk:6443 -servername nymf-b2b-soap-oio-sit09-secure.inddr.dk
  - Ved succesfuld forbindelse fås outputtet:
    - CONNECTED(00000003)
    - depth=2 OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
    - verify return:1

  - depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
  - verify return:1
  - depth=0 C = DK, ST = Herning, L = Herning, O = Skatteforvaltningen, CN = *.inddr.dk ...
- Netcat
  - Indtast følgende i terminalen: nc -zv nymf-b2b-soap-oio-sit09-secure.inddr.dk 6443
  - Ved succesfuld forbindelse fås outputtet:
    Connection to nymf-b2b-soap-oio-sit09-secure.inddr.dk (5.44.139.48) 6443 port [tcp/*] succeeded!

Browser

- Benyt Chrome eller Edge til at teste forbindelse med server
- Åben https://nymf-b2b-soap-oio-secure-sit09.inddr.dk:6443/V6.13.0/services/KvitteringHentService?wsdl
- Ved succesfuld forbindelse beder browseren om klient-certifikatet, og udstiller derefter wsdl-filen. Hvis der ikke spørges om klient-certifikatet, er dette ikke installeret korrekt.

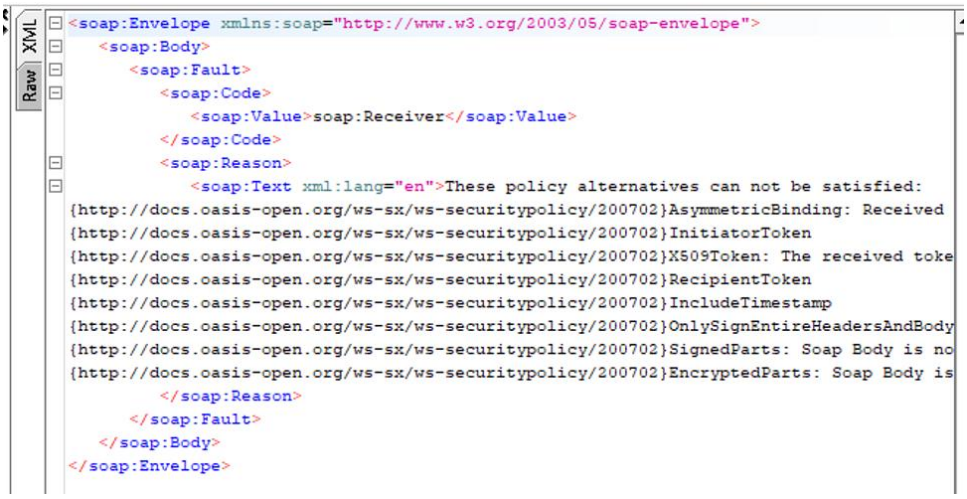
Test: kryptering af forbindelse og request (SoapUI)

Ønsker fordringshaveren at teste, at den krypterede tilslutning og kryptering af requestet er lykkedes, kan de forsøge at kalde fx KvitteringHent-servicen via NyMF-b2b. Dette gøres ved at benytte de endpoints, som er angivet i det indledende kapitel Opsætning med SoapUI.

Hvis fordringshaveren ønsker at teste den krypterede forbindelse *alene* – altså før selve requestet er krypteret – kan de udføre et service-kald, som tjekker, at der er oprettet en krypteret forbindelse til endpointet, og at der er hul igennem til dette. I SoapUI vil fordringshaveren fx kunne åbne et KvitteringHent-request og udfylde dette med relevant testmiljø, fordringshaverid, samt cvr:



Hvis fordringshaveren har forbindelse til miljøet, men endnu ikke krypteret selve requestet, fås et response som nedenstående



Hvis fordringshaveren har krypteret både forbindelse og request, vil requestet blive indsendt uden fejl.

Fordringshaverportalen

Bestil testbruger via GÆLDST/UFST
Fordringshaveren skal bestille en testbruger til Fordringshaverportalen, hvis de ønsker at benytte portalen i deres testfase. Når testbrugeren er oprettet, kan fordringshaveren tilgå Fordringshaverportalen her:

http://fordringshaverportal-sitXX.inddr.dk/

Her skal fordringshaveren klikke på "Log ind med NemID". Dernæst præsenteres en drop-down-menu, hvor fordringshaveren kan finde sig selv i bunden af menuen. Således burde fordringshaveren kunne komme på fordringshaverportalen.

Kryptering i produktion

IP-whitelistning

Bestil IP whitelistet
Når fordringshaveren går i produktion, skal de anmode GÆLDST om at få de relevante IP-adresser whitelistet mod produktion. Således bliver firewallen åbnet mod produktion.

I produktion kan fordringshaveren ikke teste, om firewallen er åbnet uden om den krypterede tilslutning. Dette skyldes, at al kommunikation med NyMF i produktion *skal* krypteres.

Kryptering af forbindelse og requests

Hent VOCES fra MitID
Lige som i test-proceduren skal fordringshaveren også i produktion bestille et fordringshaver-specifikt VOCES-certifikat. Denne gang skal VOCES bestilles fra MitID:

https://erhvervsadministration.nemlog-in.dk/

For at gøre dette skal fordringshaveren

1. Log ind på MitID Erhverv
2. Gå til certifikater/Opret certifikatprofil
3. Udfyld felterne i Stamdata
4. Vælg de services, der ønskes adgang til under Systemrettigheder
5. Udfyld felterne certifikattype, identifikation, udstedelse, mm. efter behov
6. Vælg "Opret certifikatprofil og bestil certifikat"
7. Udsted certifikat
8. Download certifikat

Hent NyMF B2B-certifikat fra GÆLDSTs hjemmeside
NyMF, produktionsserver-certifikatet downloades fra GÆLDSTs hjemmeside:

https://gaeldst.dk/fordringshaver/find-vejledning/teknisk-tilslutning-og-adgang/krypteret-tilslutning

Dette certifikat – tillige med VOCES bestilt fra MitID – er altså rettet mod produktion, og det er vigtigt, at fordringshaveren husker at tage netop disse produktionscertifikater i anvendelse frem for testcertifikaterne.

Læg certifikater i fordringshaverens system og opsæt til krypteret tilslutning
Selve processen med at lægge produktionscertifikaterne i fordringshaversystemet, samt med at opsætte fx SoapUI til den gældende TLS og WS-standard, følger de beskrivelser, der findes i kapitlet Kryptering i test. Vær dog opmærksom på, at eventuelle endpoints skal rettes mod produktion frem for test.

Registrer VOCES

Bestil oprettelse i DCS
I produktion er det en forudsætning for, at fordringshaveren kan tilslutte sig NyMF og logge på Fordringshaverportalen, at de er oprette i DCS, og at deres VOCES er registreret i TastSelv Erhverv. For at blive oprettet i DCS skal fordringshaveren kontakte GÆLDST og bede dem om at blive oprettet i DCS.

Opret systembruger i TastSelv Erhverv (registrer VOCES)
Fordringshaverens prod-certifikat skal registreres hos TastSelv Erhverv. Fordringshaveren skal gøre følgende for at registrere deres certifikat:

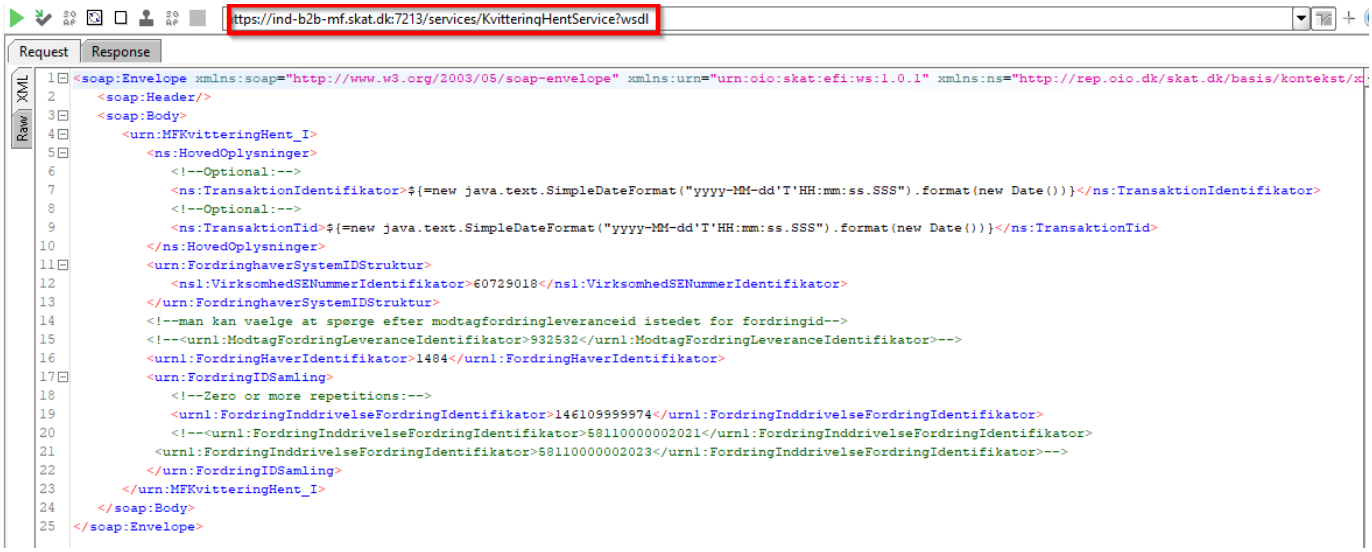
1. Log på TastSelv Erhverv som TastSelv-administrator
2. Vælg Profil- og kontaktoplysninger
3. Vælg Rettigheder og adgange til TastSelv.
4. Vælg Administrer MitID og medarbejdersignatur.
5. Vælg Tildel/fjern rettigheder, der anvendes i system-til-system-løsninger
6. Opret ny systembruger og udfyld UUID
7. Gem

Se alternativt denne guide https://info.skat.dk/data.aspx?oid=2338902

Opret rolle og tildel rettigheder i TastSelv Erhverv
Når systembrugeren (virksomhedscertifikatet) er oprettet i TastSelv Erhverv, skal fordringshaveren dernæst oprette en rolle, som er en gruppering af de rettigheder, som systembrugeren har behov for i PSRM. Rollen skal knyttes til systembrugeren i TastSelv Erhverv og skal dermed indeholde de samme informationer (CVR og UUID), som virksomhedscertifikatet indeholder.

Se guiden "Tildel systembruger til dit MitID i SKATs TastSelv Erhverv" på siden Guides til Fordringshaverportalen på gaeldst.dk.

Test: krypteret forbindelse og kryptering af request
Efter at fordringshaveren er blevet registreret i DCS og har registreret deres VOCES i TastSelv Erhverv, kan de teste forbindelse og kryptering på samme måde som i testprocessen. Dog skal port og endpoint tilpasses således, at der nu kommunikeres med produktion og ikke testmiljøet. Således vil fordringshaveren fx kunne prøve at kalde KvitteringHent-servicen via NyMF-b2b rettet mod produktion.



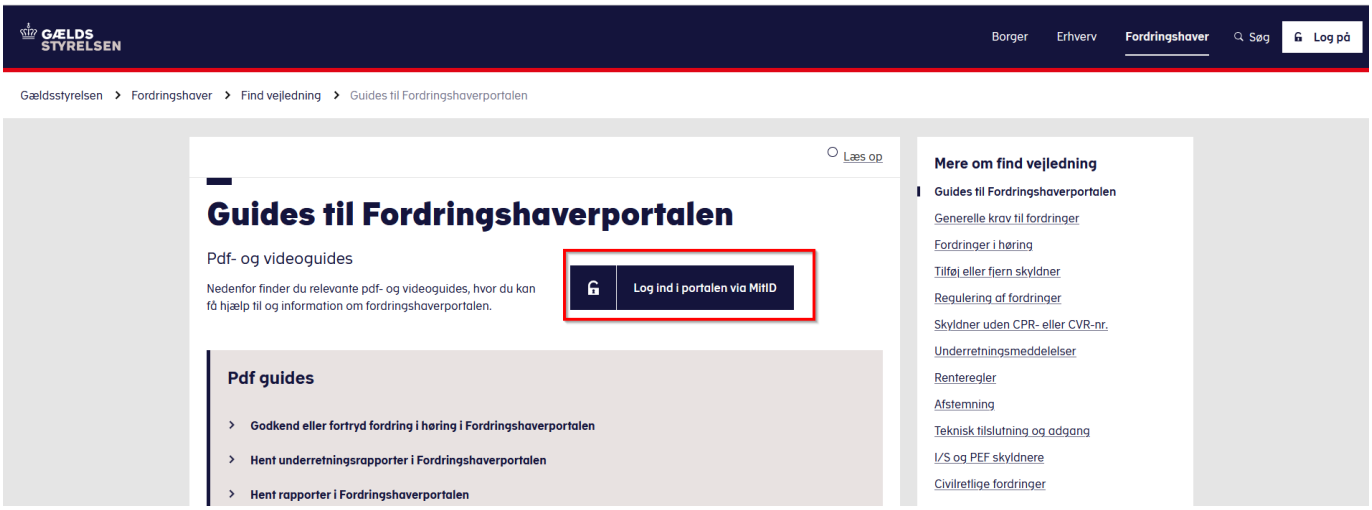

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:urn="urn:oio:skat:efi:ws:1.0.1" xmlns:ns="http://rep.oio.dk/skat.dk/basis/kontekst/x
   <soap:Header/>
   <soap:Body>
      <urn:MFKvitteringHent_I>
         <ns:HovedOplysninger>
            <!--Optional:-->
            <ns:TransaktionIdentifikator>${=new java.text.SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss.SSS").format(new Date())}</ns:TransaktionIdentifikator>
            <!--Optional:-->
            <ns:TransaktionTid>${=new java.text.SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss.SSS").format(new Date())}</ns:TransaktionTid>
         </ns:HovedOplysninger>
         <urn:FordringhaverSystemIDStruktur>
            <ns1:VirksomhedSENummerIdentifikator>60729018</ns1:VirksomhedSENummerIdentifikator>
         </urn:FordringhaverSystemIDStruktur>
         <!--man kan vaelge at spørge efter modtagfordringleveranceid istedet for fordringid-->
         <!--<urn1:ModtagFordringLeveranceIdentifikator>932532</urn1:ModtagFordringLeveranceIdentifikator>-->
         <urn1:FordringHaverIdentifikator>1484</urn1:FordringHaverIdentifikator>
         <urn:FordringIDSamling>
            <!--Zero or more repetitions:-->
            <urn1:FordringInddrivelseFordringIdentifikator>146109999974</urn1:FordringInddrivelseFordringIdentifikator>
            <!--<urn1:FordringInddrivelseFordringIdentifikator>58110000002021</urn1:FordringInddrivelseFordringIdentifikator>
          <urn1:FordringInddrivelseFordringIdentifikator>58110000002023</urn1:FordringInddrivelseFordringIdentifikator>-->
         </urn:FordringIDSamling>
      </urn:MFKvitteringHent_I>
   </soap:Body>
</soap:Envelope>
```

Fordringshaverportalen

Tildel rettigheder i TastSelv Erhverv
For at få adgang til Fordringshaverportalen, skal fordringshaveren tildele rettigheder til de relevante medarbejderes MitID-profiler. Dette gøres via SKAT TastSelv Erhverv.

Se guiden "Tildel roller og rettigheder til fordringshaverportalen i SKATs TastSelv Erhverv" på siden Guides til Fordringshaverportalen på gaeldst.dk.

Test: der kan logges på Fordringshaverportalen
Fordringshaveren bruger MitID Erhverv til at logge på Fordringshaverportalen via knappen på siden Guides til Fordringshaverportalen på gaeldst.dk.



Fejlsøgning

For at identificere fejl i løbet af tilslutningsprocessen, kan fordringshaveren fx starte deres fejlsøgning ved at genbesøge de to diagrammer i kapitlerne Flow i test og Flow i produktion. Tegningerne kan bruges dels som en forsimplet tjekliste, og dels til at identificere, hvor i processen man befinder sig, og dermed, hvor man skal fokusere sin fejlsøgning.

Hvis fordringshaveren er nået til punkt 1 i deres tilslutning til testmiljøet, og oplever problemer med at få hul igennem til endpointet, kan de fx undersøge, om den IP-adresse, de sender fra, er blandt de whitelistede, samt om det endpoint, de sender mod, angiver det korrekte testmiljø, port og snitfladeversion. Hvis fordringshaveren er nået til punkt 2-5, kan de med fordel kigge på deres certifikat og tjekke, om det er up to date, hentet fra det rette sted, af OCES 3-typen, samt om det faktisk er et test- og ikke produktionscertifikat. Derudover kan fordringshaveren kigge på selve deres opsætning af krypteringen og tjekke, at de versioner og algoritmer, som er angivet i denne guide, benyttes. Endelig, hvis punkt 8' er relevant, og der opleves problemer med Fordringshaverportalen, kan fordringshaveren evt. kontakte GÆLDST/UFST for at høre, om der skulle være problemer med Fordringshaverportalen i deres ende.

Hvis fordringshaveren er nået til punkt 1 i deres tilslutning mod *produktion* og oplever problemer med at få hul igennem til endpointet, kan de undersøge, om den IP-adresse, de sender fra, er blandt de whitelistede, samt om det endpoint, de sender mod, er rettet mod den rette port og den ønskede snitfladeversion. Hvis fordringshaveren har gennemgået punkt 2-5 og 6-7, og oplever problemer med at sende requests ind, kan de undersøge deres certifikat lidt nærmere (er det seneste produktionscertifikat, er det af OCES 3-typen, etc.), samt om der er overensstemmelse mellem informationerne i certifikat, DCS og TastSelv Erhverv. Hvis fordringshaveren har gennemgået punkt 8 og oplever problemer med at logge

på Fordringshaverportalen, skal de sikre sig, at de har fået oprettet de korrekte roller og tildelt disse til de relevante medarbejdere i TastSelv Erhverv.

For yderligere fejlsøgning, kan nedenstående cases benyttes som inspiration.

Genbrug af samme transaktionsID (også kaldet LeveranceID internt)

- Fejl: *Error Code Persistance Exception*

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
<soap:Body>
      <soap:Fault>
         <soap:Code>
            <soap:Value>soap:Receiver</soap:Value>
         </soap:Code>
         <soap:Reason>
            <soap:Text
xml:lang="en">javax.persistence.PersistenceException:
org.hibernate.exception.DataException: could not extract
ResultSet</soap:Text>
         </soap:Reason>
      </soap:Fault>
   </soap:Body>
</soap:Envelope>
```

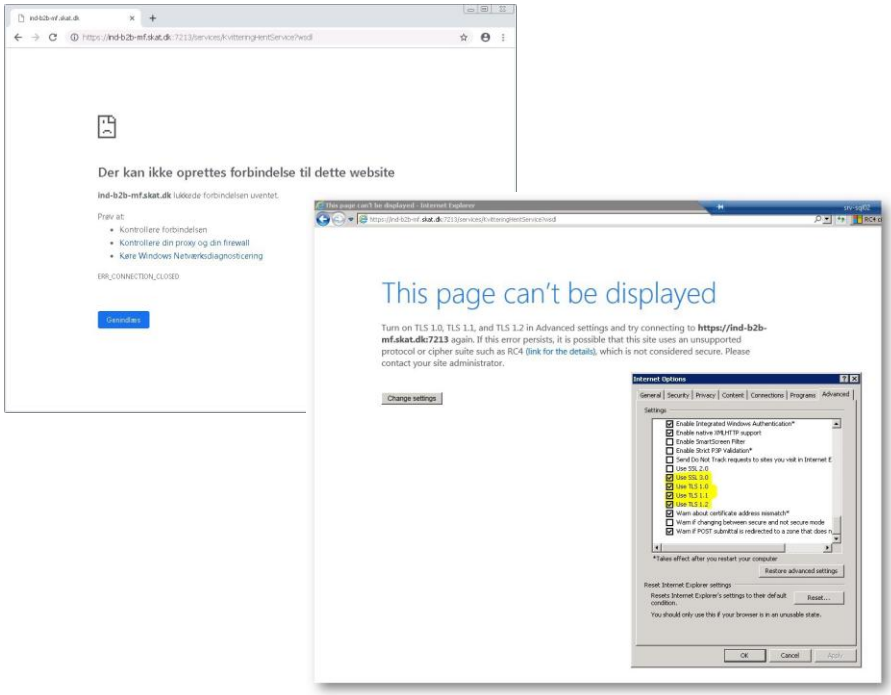
- Fejlen opstår, når man bruger det samme TransaktionsID <ns:TransaktionIdentifikator>.
- Løsningen er, at LeverenceID skal være unikt!
  Der må heller ikke genbruges gamle LeverenceID'er fra DMI.

Mangler Host Name

- Fejl: *503 Service Unavailable*
- Denne fejl kan opstå, hvis SNI (Server Name Indicator) mangler i kaldet.
- På nogle servere, eks. SAP-servere, skal SNI bevidst slås til for, at det ønskede hostnavn sendes med i requestet; ellers får man en 503 Service Unavailable.
- Se mere her
  - https://en.wikipedia.org/wiki/Server_Name_Indication
  - https://security.stackexchange.com/questions/101965/ssl3-error-when-requesting-connectionusing-tls-1-2/102018#102018
  - https://answers.sap.com/questions/473015/sap-ssl-handshake-failed.html
- Java
  - Man skal bruge Java full version 1.8.0.141 eller senere!
  - Tidligere versioner har en fejl som IKKE sender SNI med og dermed kommer man ikke længere en OpenShift miljøet; man rammer aldrig serveren og får fejl "503 Service Unavailable"

Problemer med forbindelse til produktion

- Fejl: *Der kan ikke oprettes forbindelse til dette website*



- Manglende produktionscertifikat
    - Denne fejl kan skyldes manglende produktionscertifikat på fordringshavers server
    - Sørg for at downloade det nuværende prod-certifikat for at løse denne fejl
- Hvis dette ikke løser problemet
    - Kontroller at den rigtige URL (det er mod B2B) kaldes
    - Kontroller at IP er whitelistet
    - Kontroller firewall, og bed UFST om at åbne op for porten om nødvendigt.

Manglende TastaSelv Erhverv-adgang

- Fejl: *FID is not supported* (eller fejl i *GetEntityInformation*)
- Denne fejl skyldes sandsynligvis, at man ikke har oprettet sin system-adgang i TastSelv Erhverv
- Se guiden ” Tildel systembruger til dit MitID i SKATs TastSelv Erhverv” på Gældsstyrelsens hjemmeside

NyMF er nede

- Fejl: *NyMF is down. Service not reachable*
- Når man får denne fejl, er det fordi NyMF er nede
- I produktion vil man typisk få denne fejl, hvis man har forsøgt at kalde NyMF i et servicevindue

Der stoles ikke på certifikatet

- Fejl: *A security error was encountered when verifying the message* (SoapUI) og *No trusted certs found* (OpenShift-loggen)
- Dette betyder, at der ikke stoles på certifikatet. Dette kan skyldes, at intermediate/root certificater ikke findes i truststore
- Løsning: Tjek, at certifikat-kæde er i orden.

Forkert system-id

- Fejl: *Certificate systemID does not match FordrignshaverSystemID in the message*
- Denne fejl opstår, når systemid'et i requestet ikke matcher id'et i certifikatet
- Dette skal rettes til.

SSL/TLS padding fejl

- Fejl: *getMFKvitteringHent has thrown exception…Connection has been shutdown… Invalid TLS padding data*
- Fejl i stil med denne kan opstå f.eks., hvis der gentagne gange udføres kvitteringHent-kald på et større antal fordringer.
- Fejlen kan evt. løses ved en ændring i Java.security hos fordringshaveren
    - Følgende post beskriver problemet: https://stackoverflow.com/questions/40964961/intermittent-javax-net-ssl-failure-bad-recordmac/41143041
    - En alternativ løsning er at opgradere fra Java 7 til Java 8

SoapUI får server-fejl

- Fejl: *Client received SoapFault from server*
- Denne fejl kan bl.a. skyldes
    - Hvis der er stor tidsforskel på fordringshaverens/NyMFs server. I så fald skal fordringshaveren tilpasse uret på deres server.
    - Kryptering og dekryptering virker ikke hos fordringshaveren.

Forkert symmetrisk algoritme

- Fejl: *Caused by: org.apache.wss4j.common.ext.WSSecurityException: An error was discovered processing the <wsse:Security> header*
- Denne fejl kan skyldes, at man bruger den forkerte algoritme

Forkert timestamp

- Fejl: *Caused by: org.apache.wss4j.common.ext.WSSecurityException: Invalid timestamp: The message timestamp is out of range*
- Det er et valideringstimestamp som er sat i SoapUI-headeren for at sikre, at forespørgslen ikke er kompromitteret. Det må ikke være ældre end 60 sekunder og ikke være fra fremtiden.