

Guide til krypteret tilslutning

Indholdsfortegnelse

Overblik
Certifikater
Nuværende certifikater
Certifikater, der stoles på i produktion:2
Krypteret forbindelse
Baggrundsforklaring
Hvordan trækker man et certifikat ud fra serveren 5
Yderligere sikkerhedstrin
Gensidig validering7
Eksempel:7
Eksempel på opsætning af lokalt certifikat gennem SoapUI7
Test af service-kald
TLS V1.2
WS-Policy
Keystore og truststore
Opsætning af WSS 13
Screenshot på opsætningen af et SoapUI projekt: 17
Tildele rettigheder i DCS
Debugging
Ofte opståede fejl



Overblik

For at koble på PSRM (via NyMFs B2B komponent) så skal følgende trin gennemføres:

- 1. Opret krypteret forbindelse
- 2. Tildel system-til-system rettigheder i DCS

Tidskrævende!

NB: Dette er tidskrævende og vanskelig at fejlsøge. Sørg derfor for at afsætte ekstra tid til den krypterede forbindelse - både mod test og produktion!

Certifikater

Der skal oprettes en krypteret forbindelse i forbindelse med onboarding til PSRM.

For at kunne gøre det, skal fordringshaveren benytte sig af følgende truststores, hvor test_truststore.jks (password= *password*) skal bruges til at starte med på testmiljøerne og prod_truststore.jks skal bruges, når man skal skifte til produktionen senere i forløbet:

Nuværende certifikater

Se og download tilgængelige certifikater på Gældsstyrelsens hjemmeside.

Certifikater, der stoles på i produktion:

Hvis jeres VOCES-certifikat er en af nedenstående, så stoles der automatisk på jeres certifikat, og der skal derfor ikke tilføjes noget til truststoren.

- Alias name: trust2408 oces ca iv (trust2408 oces primary ca)
- Alias name: trust2408 oces primary ca
- Alias name: trust2408 oces ca iii (trust2408 oces primary ca)
- Alias name: trust2408 oces ca ii
- Alias name: trust2408 oces ca v (trust2408 oces primary ca)



Krypteret forbindelse

Baggrundsforklaring

Keystore:

- Indeholder private/public key par for certifikater.
- Benyttes til at signere og validere, dvs. at identificere en afsender.
- Information som er signeret (=krypteret) med den private nøgle kan kun valideres (deprypteres) med den tilhørende offentlige (=public) nøgle.
- Man kan eksportere sin public key og dele den med alle, men private key må aldrig sendes ud til andre. Den skal holdes hemmelig.

Truststore:

- Indeholder eksterne navne (public keys/certifikater) på dem man stoler på.
- Truststoren bruges til at kryptere med således at beskeden ikke kan læses af andre undervejs.
- Information som er krypteret med den offenlige (=public) nøgle kan kun deprypteres med den tilhørende private nøgle.

Man har dermed brug for et VOCES-certifikat, som skal bestilles fra NETS.

I første omgang skal der bruge et test-certifikat, som kan hentes herfra <u>https://www.nets.eu/dk-da/kundeservice/nemid-tjenesteudbyder/NemID-tjenesteudbyderpakken/Pages/OCES-II-certifikat-eksempler.aspx</u> (det første gyldige Virksomhedscertifikat på siden downloades - bemærk password= *Test1234*) Dette kan bruges til test, indtil man får udstedt sit eget certifikat.

VOCES-certifikatet bruges sammen med test-Truststore.jks til hhv. at signere og kryptere med.



Følgende tegning illustrerer flowet:



- 1. Fordringshaver: Bruger egen private key fra Keystore til at signere med.
- 2. Fordringshaver: Bruger NyMFs public key fra Truststore til at kryptere med.
- 3. Fordringshaver: Sender fordring.
- 4. NyMF: Bruger egen private key til at dekryptere med.
- 5. NyMF: Bruger egen public key (men kun udsteder delen) til at validere med.



Hvordan trækker man et certifikat ud fra serveren

Man kan forbinde og trække certifikatet ved kommandoen her:

Kommando til at trække certifikat

```
openssl s_client -showcerts -connect nymf-b2b-soap-oio-dockXX-
secure.inddr.dk:443 -servername nymf-b2b-soap-oio-dockXX-secure.inddr.dk
</dev/null 2>/dev/null|openssl x509 -outform PEM >clientTrustCert.pem
```

Man kan også få vist certifikatet sammen med andre egenskaber med følgende kommando:

```
openssl s client -connect <ip>:<port> -servername <ip>
```

Erstat *<ip>* and *<port>* med url på den server du kommunikerer med. Kommandoen kan køres i Unix eller i Windows gennem fx Cygwin eller Git Bash. Ved forbindelse listes bl.a. serverens test-certifikat.



Eksempel:

Brug altid det docker miljø, I har fået tildelt.

I må ikke sende fordringer ind på andre miljøer end det miljø, der er tildelt til jer.

openssl s_client -connect <u>nymf-b2b-soap-oio-dockXX.inddr.dk</u>:443 -servername <u>nymf-b2b-soap-oio-dockXX-secure.inddr.dk</u>



Herefter kan der forbindes til testmiljøet gennem servicen FordringIndberetService. Det kræver et par yderligere sikkerhedstrin, som vi gennemgår nedenfor.

Yderligere sikkerhedstrin

NyMF kræver, at klienter krypterer beskeder. Der skal udveksles certifikater, så NyMF kan tilføje dem til truststore. Klienter krypterer deres trafik med VOCES-certifikat, hvor CVRnummer i certifikatet skal stemme overens med indberetters CVR-nummer.

Man kan desuden finde sit CVR-nummer på sit VOCES-certifikat ved at følge følgende skridt:



- 1. Hent og installer en keystore applikation til at håndtere certifikater. Vi bruger selv "keystore explorer" <u>http://keystore-explorer.org/downloads.html</u>
- 2. Åbn dit certifikat og dobbeltklik på det. Her kan du se dit Root-, Intermediate- og Usercertifikat:
- 3. Tryk på User-certifikat (den nederste i hierarkiet).
- 4. Tryk på notesbogen
- 5. Aflæs dit CVR- og UID-nummer.



Gensidig validering

For at oprette system-til-system-adgang til PSRM, skal virksomheden have et validt OCES-II certifikat. For alle services tillades VOCES (Virksomheds) certifikat. Det anbefales at bestille sit virksomhedscertifikat hos NETS. Indtil man får sit eget certifikat, kan man bruge NETS test-certifikat herfra: <u>https://www.nets.eu/dk-da/kundeservice/nemid-tjenesteudbyder/NemID-tjenesteudbyderpakken/Pages/OCES-II-certifikat-eksempler.aspx</u>

Vi benytter certifikaterne listet øverst på siden i prod og test-miljøer.

Eksempel:

Lokal certifikat gennem SOAPUI

Eksempel på opsætning af lokalt certifikat gennem SoapUI

Hent det gyldige test cerifikat (det første virsomhedscertifikat under <u>https://www.nets.eu/dk-da/kundeservice/nemid-tjenesteudbyder/NemID-tjenesteudbyderpakken/Pages/OCES-II-certifikat-eksempler.aspx</u>).



Når certifikatet er hentet, kan det sættes op med eksempelvis SoapUI:



HTTP Settings	KeyStore	Cillses ha Destan cets VOCES addia n12	Browse
Proxy Settings	- Reystore.	Citosestoj (censtro co_gynagozz	
SSL Settings	KeyStore Password:	•••••	
WSDL Settings	Enable Mock SSL:	enable SSL for Mock Services	
UI Settings	Mark Port		
Editor Settings	MOCKFOR		
Tools	Mock KeyStore:		Browse
WS-I Settings	Mock Password:		
Global Properties			
Global Security Settings	Mock Key Password:		
WS-A Settings	Mock TrustStore:		Browse
Global Sensitive Information Tokens	Mack TructStore Dassword		
Version Update Settings	mock musistore rassmoru.		
AlertSite Connector Plugin	Client Authentication:	requires client authentication	



Certifikatets password findes på siden, det er hentet fra (Test1234)

Test af service-kald

Opret forbindelse til servicen FordringIndberetService:

For docker-miljøer er det følgende service, man skal kalde: <u>https://nymf-b2b-soap-oio-dockXX-</u> secure.inddr.dk/services/FordringIndberetService?wsdl, hvor XX skal erstattes med det dockernummer man har fået.

SOAP P	roject ×
New SOAP Proj Creates a WSDL	ect /SOAP based Project in this workspace
Project Name:	XXX.XXX.XXX
Initial WSDL:	s://XXX.XXX.XX.XX:7213/services/FordringIndberetService?wsdl Browse
Create Requests	Create sample requests for all operations?
Create TestSuite	Creates a TestSuite for the imported WSDL
Relative Paths:	Stores all file paths in project relatively to project file (requires save)
0	OK Cancel
Send nu et requ	est. Sørg for at pege på den udgående trafik mod HTTPS endpoint:



		e u
	I GI D & II II I III III III III IIII II	
	<pre>bit bit bit bit bit bit bit bit bit bit</pre>	<pre>inter testing tes</pre>
÷.		
*	Hader II Machiner II WA WARM PERSONA APPropriate	Theater (5) Attachment (5) \$2 Mo () cards and a second
	tution (1780) Bytes()	

Ved forbindelse til miljøet fås et response som ovenstående. Egentlige indberetninger kræver kryptering af requestet. Derfor skal vi nu opsætte certifikater og nøgler for in-going og out-going beskeder. Disse gøres nedenunder:

Transport Layer Security (TLS)

TLS V1.2

For at sikre at data udveksles efter sikre, velafprøvede principper, og fuldt krypterede kanaler, benyttes HTTP over TLS. Det kun tilladt at forbinde til NyMF ved at benytte nyeste TLS version (TLS v1.2).

Desuden er der begrænsning på, hvilke ciphers, der er tilladt. NyMF er konfigureret til at <u>afvise</u> forbindelser, der anvender følgende ciphers:

• 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

SoapUI opsætning til TLS v1.2

Serveren understøtter kun TLS v1.2, som SoapUI skal konfigureres til:

- 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=TLSv1.2"
- 4. Genstart SoapUI

Web Service Security (WSS)

Web Services Security (WSS) krypterer indholdet og sørger for en sikker kommunikation med web services i PSRM.

WS-Policy

NyMF kræver, at indholdet af beskeden anvender følgende WS-Policy:

WS-Policy

```
<?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-</pre>
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-</pre>
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:TripleDes/>
              </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>
```

I grove træk betyder det, at klienter forventes at:

- Indsætte tidsstempel.
- Signere besked ved brug af samme certifikat som SSL-forbindlesen (signatur algoritme: RSA_SHA1, Canonicalization: xml-exc-c14n, digest: sha1). Både body og tidsstempel signeres.
- Kryptere besked ved at anvende NyMF's offentlige certifikat (Symmetrisk algoritme: tripledes-cbc, nøglealgoritme: rsa-oaep). Kun body krypteres.



Keystore og truststore

SoapUI skal sættes op til kryptering og dekryptering af beskeder sendt over B2B med WSS. Det sker med client keystore og truststore.

Det tidligere hentede virsomhedscertifikat kan bruges som keystore, men der er også brug for et truststore til den offentlige del af servercertifikatet.

a) Som udgangspunkt kan truststore øverst på denne side benyttes: test_truststore.jks. (Et tilsvarende findes for PROD når man kommer så langt og skal koble på produktionen.)

Brug "password" som kodeord for at komme ind. Alternativt kan man selv oprette et truststore. Processen er beskrevet her:

Opsætning af TrustStore (valgfri)

Denne guide kan følges, hvis det ovenstående truststore ikke kan bruges. Guiden forudsættes, at du benytter et linux-miljø. Både Java og OpenSSL skal være installeret. Windows kan også benyttes, men da kan openssl-kommandoerne ikke nødvendigvis bruges.

1) Download det offentlige certifikat fra endpoint:

 $openssl\ s_client\ -showcerts\ -connect\ <ip>:<port> </dev/null\ 2>/dev/null|openssl\ x509\ -outform\ PEM\ >clientTrustCert.pem$

Erstat <ip> and <port> med den server, du kommunikerer med.

2) Opret JKS truststore, der indeholder certifikatet:

keytool -import -file clientTrustCert.pem -alias trustedServer -keystore clientTrustStore.jks -deststoretype JKS -storepass password. Indtast yes, hvis der spørges til certifikatets autenticitet

Opsætning af WSS

Efter ovenstående trin kan der i kommunikeres med serveren. Ved request får man en fejlmeddelelse i stil med *A security error was encountered when verifying the message*, hvis requestet ikke er krypteret. Det kan forhindres af WSS.

Opsætning af indgående og udgående kryptering og dekryptering i SoapUI

1. Dobbeltklik på dit SoapUI-projekt (folderen der er higlightet i blå):

FordringIndberetService?wsdl

🖶 🔁 MFFordringIndberetServiceBinding

🖮 컱 MFFordringIndberetServicePortType



Overview TestSuite	s WS-Secur	ity Configuration	s Security Scan Defau	llts	
Outgoing WS-Security	y Configuratio	ns Incoming V	VS-Security Configuratio	ns Keystores T	ruststores
	Name			Default Username/Al	ias
Gå til Keystores	s, og impo	orter både v	irksomhedscerti	fikatet (VOCI	ES, password
est1234) og ch	ient i rust.	store.jks (pa	asswordet er pa.	sswora):	
Overview TestSuite	es WS-Secu	irity Configuratio	ons Security Scan De	faults	
Outgoing WS-Securit	ty Configurati	ons Incoming	JWS-Security Configura	ations Keystores	Truststores
+ ×					
Source	a n12 (Status	Password	Default Alias	Alias Password
	gipiz ()K			
C:\temp\test_truststor	ejks v				
C:\temp\test_truststor	assword s p til outg Service?wsdl es \ WS-Secr	kal ikke fyl oing WS-se	Ides ud. curity configura	ition: aults	
C:\temp\test_truststor C:\temp\test_truststor Cilføj <i>Timestam</i> FordringIndberet Overview TestSuit Outgoing WS-Securi + ×	assword s p til outg Service?wsdl es WS-Sect ty Configurati	kal ikke fyl oing WS-sec urity Configuratio	Ides ud. curity configurations Security Scan Def WS-Security Configurat	aults	Truststores
C:\temp\test_truststor Lias og alias po Cilføj Timestam FordringIndberet Overview TestSuit Outgoing WS-Securi + ×	assword s p til outg Service?wsdl es WS-Seco ty Configurati	kal ikke fyl oing WS-se urity Configuratio	Ides ud. curity configura ons Security Scan Def WS-Security Configurat	ition: aults tions Keystores Default Username/	Truststores 'Alias
C:\temp\test_truststor Lias og alias po `ilføj <i>Timestam</i> FordringIndberet Overview TestSuit Outgoing WS-Securi + × out	assword s p til outg Service?wsdi es WS-Seco ty Configurati Name	kal ikke fyl oing WS-sec urity Configuratio	Ides ud. curity configurations Security Scan Def	ution: aults iions Keystores Default Username/	Truststores 'Alias
C:\temp\test_truststor C:\temp\test_truststor Cilføj Timestam FordringIndberet Overview TestSuit Outgoing WS-Securi + × out	assword s p til outg Service?wsdl es WS-Secu ty Configurati Name	kal ikke fyl oing WS-se urity Configuratio	Ides ud. curity configura ons Security Scan Def WS-Security Configurat	aults ions Keystores Default Username/	Truststores Alias
C:\temp\test_truststor lias og alias po ilføj Timestam FordringIndberet Overview TestSuit Outgoing WS-Securi + × out • • • • • •	assword s p til outg Service?wsdi es WS-Sect ty Configurati Name	kal ikke fyl oing WS-sec urity Configuratio	Ides ud. <i>curity configura</i> ms Security Scan Def WS-Security Configurat	ution: aults ions Keystores Default Username/	Truststores 'Alias



4. Tilføj Signature:

Timestamp		Keystore	VOCES avid	0.032 -		
agnature	-				14. J. 2	
		Alias	nets_danid_a	/stu_voces_gyl	dig .	
		Password:				
		Key Identifier Type:	Binary Securi	ty Token	•	
		Signature Algorithm	http://www.	n3.org/2000/09/si	nidsig#rsa-shal	
		Signature Canonicalization:	http://www.	-3.org/2001/10/w	mi-exc-c14n#	
		Digest Algorithm:	http://www.w3.org/2000/09/vm/dsig#sha1			
		Use Single Certificate:	🗌 Use single	certificate for sig	ning	
		Custom Key Mathles				
		Contorn Key Identifier VelorType Parts:				
			+ ×			
			10	Name	Namespace	Encode
			S	Timestamp	http://docs.o	Content
				Body	http://schem	Content

Sørg for at vælge *Binary Security Token* under *Key Identifier Type*. De valgte algoritmer <u>skal være identiske</u> med dem i screenshot ovenfor! Signature password er VOCES-certifikatets password (Test1234) Under *Parts* indtastes nedenstående information:

ID	Name	Namespace	Encode
	Timestamp	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss- wssecurity-utility-1.0.xsd	Content
	Body	http://www.w3.org/2003/05/soap-envelope	Content

5. Tilføj kryptering:

Timestamp	Keystore:	test_truststore.jks 💌				
sagnature Encryption	Aliasi	inddr 🔻				
	Passwordt					
	Key Identifier Type:	Binary Security Token 💌				
	Embedded Key Name					
	Embedded Key Plessorid					
	Symmetric Encoding Algorithm	http://www.w3.org/2001/04/xmienc#tripledes-cbc http://wwww.w3.org/2001/04/xmi				
	Key Encryption Algorithm:					
	Create Encrypted Keylo	Indicates whether to encrypt the symmetric key into an EncryptedKey or not				
	Parts	+ ×				
		ID Name Namespace Encode				
		Body http://www.w Content				
2	1 1 1 1					



Body http://www.w3.org/2003/05/soap- envelope Content Sørg for at vælge Binary Security Token under Key Identifier Type. De valgte algoritmer <u>skal være identiske</u> med dem i screenshot ovenfor! Tilføj indkommende dekryptering: Image: Security Configurations Security Scale Security Configurations Outgeing WS-Security Configurations Security Scale Security Configurations Reguters Image: Name Decopt Keystore Signature Keystore Password Image: Name Decopt Keystore Teststores Password Det indkommende password er VOCES' password (Test1234). Eequest-editoren, (dobbeltklik Request1, markeret blåt nedenfor): MFFordringIndberetServicePortType SettiffFordringIndberet Signature Keystore Password Styptering og dekryptering til beskeder: No Authorization No Authorization Not Yet Configured Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	ID	Name		Namespace		Encode			
Sørg for at vælge <i>Binary Security Token</i> under <i>Key Identifier Type</i> . De valgte algoritmer <u>skal være identiske</u> med dem i screenshot ovenfor! Tilføj indkommende dekryptering: Overview TesSuite WS-Security Configurations Security San Defaults Outgoing WS-Security Configurations Security San Defaults WS-Security Configurations Incoming WS-Security Configurations WS-Security Configurations Regators Det indkommende password er VOCES' password (Test1234). equest-editoren, (dobbeltklik <i>Request1</i> , markeret blåt nedenfor): MFFordringIndberetServicePortType getMFFordringIndberet Signequest1 kryptering og dekryptering til beskeder: No Authorization Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.		Body	http://ww envelope	/w.w3.org/2003/05	<u>/soap-</u>	Content			
Outgoing WS-Security Configurations Incoming WS-Security Configurations Trustatores Image: Name Decrypt Keystore Signature Keystore Password Image: Name VOCES_gyldig.pl2 text_trustatore.jks Password Image: Name VOCES_gyldig.pl2 text_trustatore.jks Password Det indkommende password er VOCES' password (Test1234). Equest-editoren, (dobbeltklik <i>Request1</i> , markeret blåt nedenfor): MFFordringIndberetServicePortType Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signature Keystore Image: Signatu	Sørg De va Tilfø	for at v algte alg j indkor	vælge <i>Bina</i> goritmer <u>s</u> mmende d	ury Security Token kal være identiske lekryptering:	under <i>I</i> med de	Key Identi em i scree	i <i>fier Typ</i> enshot o	pe. wenfor!	
Outgoing WS-Security Configurations Keystore Trustatore Name Decrypt Keystore Signature Keystore Password Name VOCES_gyldig.pl2 test trustatore.jls Password Det indkommende password er VOCES' password (Test1234). equest-editoren, (dobbeltklik <i>Request1</i> , markeret blåt nedenfor): MFFordringIndberetServicePortType getMFFordringIndberetServicePortType getMFFordringIndberet % % Request1 kryptering og dekryptering til beskeder: Muthorization No Authorization Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	Overvie	ew resisu	ites wo-securit	security scal	n Delauits				
Name Decrypt Keystore Signature Keystore Password in VOCES_gyldig.p12 test_trustore.jks Password Det indkommende password er VOCES' password (Test1234). equest-editoren, (dobbeltklik <i>Request1</i> , markeret blåt nedenfor): MFFordringIndberetServicePortType getMFFordringIndberet in in No authorization No Authorization Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	Outgo	ing WS-Secu	rity Configuration	Incoming WS-Security Confi	igurations	Keystores Tr	uststores		
in VOCES_gyldig.p12 test_truststore.jks Det indkommende password er VOCES' password (Test1234). equest-editoren, (dobbeltklik <i>Request1</i> , markeret blåt nedenfor): MFFordringIndberetServicePortType getMFFordringIndberet 30 Request1 kryptering og dekryptering til beskeder: Authorization No Authorization Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	+ ×	Nam	e	Decrypt Keystore		Signature Keys	store	Pas	sword
Det indkommende password er VOCES' password (Test1234). equest-editoren, (dobbeltklik <i>Request1</i> , markeret blåt nedenfor): MFFordringIndberet getMFFordringIndberet Request1 kryptering og dekryptering til beskeder: Authorization: No Authorization No Authorization No Authorization Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	in		,	VOCES_gyldig.p12	test_tru	ststore.jks		•••••	
Authorization: No Authorization Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	MFFord Ø getl	-editore IringIndb MFFordri Request	en, (dobbel eretServiceP ngIndberet 1	ltklik <i>_Request1</i> , ma ortType	urkeret	blåt neder	nfor):		
No Authorization Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	MFFord Ø getl Sp krypte	-editore IringIndb MFFordri Request ering og	en, (dobbel eretServiceP ngIndberet 1 dekrypter	tklik <i>Request1</i> , ma ortType ring til beskeder:	rkeret	blåt neder	nfor):		• 0
Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	MFFord G gett krypte	-editore IringIndb MFFordri Request pring og	en, (dobbel eretServiceP ngIndberet 1 dekrypter	tklik <i>Request1</i> , ma ortType ring til beskeder:	rkeret	blåt neder	nfor):		•0
Add New Authorization Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	MFFord gett krypte	-editore IringIndb MFFordri Request ering og	en, (dobbel eretServiceP ngIndberet 1 dekrypter No Au No Au	tklik <i>Request1</i> , ma ortType ring til beskeder: thorization		blåt neder	nfor):		•0
Not Yet Configured Authorization has not been set for protected services. Use the Authorization drop down to configure.	Authoriz	-editore IringIndb MFFordri Request ering og	en, (dobbel eretServiceP ngIndberet 1 dekrypter No Au No Au	tklik <i>Request1</i> , ma ortType ring til beskeder: thorization		blåt neder	nfor):		•0
	Authoriz	-editore IringIndb MFFordri Request ering og	en, (dobbel eretServiceP ngIndberet 1 dekrypter No Au No Au Add N	tklik <i>Request1</i> , ma ortType ting til beskeder: thorization thorization		blåt neder	nfor):		•0
	Authoriz	-editore IringIndb MFFordri Request ering og	en, (dobbel eretServiceP ngIndberet 1 dekrypter No Au No Au Authoriz Use ti	tklik <i>Request1</i> , ma ortType ring til beskeder: thorization w Authorization Not Yet Confi ation has not been set he Authorization drop	gured for prot	ected servio	ces.		
	Authoriz	-editore IringIndb MFFordri Request ering og	en, (dobbel eretServiceP ngIndberet 1 dekrypter No Au No Au Add N	Itklik <i>Request1</i> , ma ortType ring til beskeder: thorization ew Authorization Not Yet Confi ation has not been set he Authorization drop	gured for prot	ected servio	nfor):		

Vælg Basic:



Add Authorization		
Add Authorization		
Туре:	Basic	
0	OK Cancel	
ælg ind- og udgåe	nde kryptering:	
Authorization: B	isic	
Username:		
Password:		
Domain:		
Pre-emptive auth:	 Use global preference 	
	O Authenticate pre-emptively	
Outgoing WSS:	out 💌	
Incoming WSS:	in 💌	

Screenshot på opsætningen af et SoapUI projekt:

- 1. Download og importér en SoapUI-fil.
- 2. Husk at omdøbe IP-adressen:



Tildele rettigheder i DCS

For at få system-til-system adgang skal fordringshaver tildele den korrekte rettighed i Det Centrale Sikkerhedssystems (=DCS).

CVR-nummer og UID fra certifikatet skal være oprettet i DCS.

Se guiden "Systembrugeroprettelse ved SKATs Tastselv" på Gældsstyrelsens hjemmeside.

Baggrund:

Når der sendes et request ind, tjekkes der i DCS for at se, om fordringshaver har ret til at benytte system-til-system-løsningen. Derfor skal en Administrator/Systembruger i DCS tildele de korrekte rettigheder til de individuelle medarbejdere. DCS tilgås via SKAT TastSelv Erhverv.

Debugging

Når SOAPui error log er mangelfuld kan man også finde en mere detaljeret log via Openshift loggen for det respektive miljø (udskift XX i linket med dock nummeret - <u>https://openshift.inddr.dk:8443/console/project/dockXX/browse/pods/nymf-b2b-1-</u> <u>216sz?tab=logs</u>

Eksempel Dock25

9874	
14215	
. 5414	Constitution and the service provided investigation of the service of some body is not signed.
5.577	Control and a second state of the second state
1876	at org.spethe.orf.en.pull(y.Assertionin/Orap.checkffectivePull(y(Assertionin/Orap.javai179)
19478	<pre>st org.spache.csf.wt.policy.PolicyWrificationInterceptor.handls(PolicyWrificationInterceptor.java:802)</pre>
	at org.apache.cxf.wn.policy.AbstractPolicyInterceptor.handlefessage(AbstractPolicyInterceptor.java:44)
	at org.speche.caf.phase.PhaseInterceptorChain.doIntercept(PhaseInterceptorChain.java:300)
	at org.apathe.csf.transport.ChainEnitiationOnserver.owHestage(ChainEnitiationOnserver.java:121)
	at org.apathe.csf.transport.http://bstractHTPDestination.invoke(AbstractHTPDestination.java;254)
1004	at org.apache.cxf.transport.http_jetty.letty#TFFGestimatios.doService(letty#TFFGestimatios.java;234)
1481	at org.apache.cvf.transport.http_jetty.JettyHTPMandiar.Aandie(JettyHTPMandiar.java)70)
3444	at org.eclipse.jetty.server.handler.ContextNandle(ContextNandler.jana:1129)
74527	at srg.eclipse.jetty.server.handler.ContextMandler.dolcope(ContextMandler.java:1065)
13,222	at seg.eclipse.jetty.server.handler.ScopedNandler.handle(ScopedNandler.java:34)
1488	at org.eclipse.jetty.server.hamiler.ContextHamilerCollection.hamile(CantextHamilerCollection.java:235)
1000	at org.eclipse.jetty.server.handler.HandlerWrapper.handlerWrapper.java:97)
3483	at org.eclipse.jetty.server.Jever.favale(Server.java(499)
3483	at org.eclipse.jetty.server.HttpChennel.Amodie(HttpChennel.java:311)
3483	at org.eclipse.jetty.server.HttpConnection.onfillableDHttpConnection.java/257)
5284	at org.eclipse.jetty.io.AbstractConnectionEz.rus(AbstractConnection.java:544)
10400	at org.eclipse.jetty.utll.thread.QueueEThreadPool.runlob(QueuedThreadPool.jeus:635)
1414	at arg.eclipse.jetty.util.thread.QueuedThreadPuol33.run(QueuedThreadPuol.Sava:SSS)
10003	at jeve.lang.Thread.run(Thread.jeve:745)
5498	11-22-2019 39:38:15.313 (stp1007590108-600) 4000 595178 - 2019-13-12709/38-15.3132(595178)4000(201004170778/932-5913-404-426-0100754c6es);10.328.7.35;eper-52
5688	(qtp1007590166-600) Soup12/multOxtInterceptor DWO class org.apathe.csf.binding.soup.interceptor.Soup12/multOxtInterceptorSoup12/multOxtInterceptorInternal

Ofte opståede fejl

Det er muligt SoapUI skal genstartes efter man har fået sat ovenstående indstillinger op.



Genbrug af samme transaktionsID (også kaldet LeveranceID internt): **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 den skal være unik.

NB! LeverenceID skal være unikt! Der må heller ikke genbruges gamle LeverenceID'er fra DMI.

[∼] 503 Service Unavailable: Mangler Host Name

SNI in SAP server

503 Service Unavailable

Denne fejl kan opstå, hvis SNI mangler i kaldet. SNI = Server Name Indicator

På nogle servere, eks. SAP servere, skal SNI bevidst slåes 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

<u>Java:</u>

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"

* Manglende produktionscertifikat hos fordringshaveren

Følgende fejl:



Skyldes manglende produktionscertifikat på fordringshavers server.

Se afsnit "Hvordan trækker man et certifikat ud fra serveren?" ovenover.

^{*} Fejlbesked: A Security error was encountered when verifying the message



Hvis fordringshaveren møder følgende fejlbesked: An unsecured or incorrectly secured fault was received from the other party - A Security error was encountered when verifying the message, så kan det skyldes følgende:

- Undersøge med operations om b2b komponenten er ens på de to servere hvor disse er deployed
- Undersøge med operations om de to servere hvor b2b komponenten er deployed på er deployed ens og på samme tidspunkt-ish.
- Sikre at truststoren indeholder de certifikater der skal til for at der stoles på kommunikationen (ved virksomhedscertifikater fra TRUST 2048, så gælder dette intermediate og rod-certifikatet)

[∼] FID is not supported

Når man kalder ind mod PROD kan man få fejlen: "FID is not supported" alternativt noget med fejl i GetEntityInformation.

Det er fordi man ikke har oprettet sin system-adgang i TastSelv-Erhverv.

Se guiden "Systembrugeroprettelse ved SKATs Tastselv" på Gældsstyrelsens hjemmeside.

* NyMF is down. Service not reachable

Når man får denne fejl, er det fordi NyMF er nede.

PROD: Man vil typisk få den, hvis man har forsøgt at kalde NyMF i et servicevindue. Man skal benytte korrekt procedure for at undersøge, hvilke aktioner, der er gået igennem.

Dette er beskrevet her: IndberetfordringService fejlhåndtering

^w No trusted certs found

Fejlen set fra FH:

Mar 22, 2019 2:55:09 PM dk.dsb.igp.secure.lib.ThirdPartySecurity postMessage

SEVERE: <?xml version="1.0" encoding="UTF-8" standalone="no"?><soap:Envelope xmlns:soap="<u>http://schemas.xmlsoap.org/soap/envelope/</u>"><soap:Body><soap:Fault><faultcode xmlns:ns1="<u>http://ws.apache.org/wss4j</u>">ns1:SecurityError</faultcode><faultstring>A security error was encountered when verifying the message</faultstring></soap:Fault></soap:Body></soap:Envelope>



<soap:Envelope

xmlns:soap="<u>http://schemas.xmlsoap.org/soap/envelope/</u>"><soap:Body><soap:Fault><faultcode xmlns:ns1="<u>http://ws.apache.org/wss4j</u>">ns1:SecurityError</faultcode><faultstring>A security error was encountered when verifying the message</faultstring></soap:Fault></soap:Body></soap:Envelope>

javax.xml.soap.SOAPException: A security error was encountered when verifying the message

Fejl fundet i loggen: Openshift -> dock38-> pods->nymf-b2b



No trusted certs found

Det betyder, at der ikke stoles på certifikatet. Dette er sikkert, fordi intermediate/root certificater ikke er i truststore.

Løsning:

Få certifikat fra FH, tjek deres certifikat kæde:



📃 Certificate	×
General Details Certification Path	
Certification path TRUST2408 OCES Primary CA	
Certificate status: This certificate is OK.	View Certificate
	OK

Hent truststore og kontroller det:

Fra github:

Åben truststore med Keystore explorer (det er lettere end kommandoer)

Password er: storepass



1+		1.4	·····································	10.6				
-	e'Trae	reter	ede #					
л	8	Ξ	Entry Rane	Algorithm	Ney Size	Certificate Expiry	Last Modified	
8	۰.		0581-85	RSA	4095	12301/2037 10.02.14 CET	12/0-1/2017 17:19:47 CET	
×	1	٠	id-tect-echaeni	RSA	2048	24/10/3011 09.33.36 CEST	00/03/2017 15.22.51 CET	
*	10	٠	left.	RSA	2248	27/02/2029 09.23.10 CET	06/04/2017 11:50-44 CEST	
я.	+		int_nevi	REA	2048	04/07/2012 08:48:43 CEST	18/12/2018 12:22.35 CET	
*	÷	٠	trust2408 scale calil (trust2408 scale primary cal)	RSA	2040	14/05/2029 11.15.53 CEST	25/03/2019 30.46.06.CET	
۰		٠	trust2408 eces caliii (trust2408 oces primary ca)	RSA	2246	36/10/2532 14.07.40 CEIT	25/99/2016 13.36.23 CEST	
2		٠	trust2408 acres primary ca	RSA	4096	03/12/2037 14.11.34 CET	25/99/2018 13:36.16 CEST	

Check at intermediate og root certificates er i store.

Hvis de ikke er, tilføj dem dertil.

Dette gøres ved at trykke View Certificate i ovenstående billede af FH-certifikat på intermediate og vælg Details \rightarrow Copy To file \rightarrow P7B format.

Inde i Keystore explorer Tools \rightarrow add trusted certs

Lav en ny branch, commit din nye truststore, opret pull request, få reviewet og merge ind.

Kør release-nymf	Project Release-ici-nymf-integration
Releaseall	Project ReleaseAll
Docker deploy nymf-b2b	Docker - Deploy - nymf-b2b

All good.

* Certificate systemID does not match FordrignshaverSystemID in the message

Denne fejl kommer når systemid i beskeden ikke matcher det i certificatet.

Her er eksempel med DSB:

Det er pga. at denne værdi skal matche med subject værdien i certifikatet.

<urn:FordringhaverSystemIDStruktur>

 $<\!ns1:VirksomhedSENummerIdentifikator\!>\!25050053<\!/ns1:VirksomhedSENummerIdentifikator>$



</urn:FordringhaverSystemIDStruktur>

Certifikatet

💼 Certificate	×
General Details Certification Path	
Show: <all></all>	\checkmark
Field	Value ^
Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from Valid from Valid to Subject Public key SERIALNUMBER = CVR:25050053-0 CN = DSB - IGP - Test O = DSB // CVR:25050053 C = DK	574ccfae sha256RSA sha256 TRUST2408 OCES CA II, TRUS 6. juni 2017 11:27:32 6. juni 2020 11:16:39 CVR:25050053-UID:60891593 RSΔ (2048 Bits)
E	lit Properties
	ОК

Dette skal fordringshaver rette til. Er det for test, kan man rette SystemIndberetternummeret i fordringshaveraftalen på testmiljøet f.eks. til Nets certifikatet (som man typisk vil bruge til test)

[~] Nægtede at oprette forbindelse

Hvis der ikke er forbindelse med denne fejlbesked. (taget fra Metros onboarding, da de prøvede at forbinde fra deres PROD miljø til vores prod miljø.)



Laite F.
9 9 I

- Kontroller at de kalder på den rigtige URL(det er mod B2B). PROD
- Kontroller at deres IP er whitelistet (spørg Operations, eller fremfind case på toolkit <u>https://goto.netcompany.com/cases/GTO587/SKMICI/Lists/Tasks/AllItems.aspx</u>)
- Spørg Operations om de har modtaget pakker fra deres IP (de vil gerne have et tidspunkt fra hvornår adgang er forsøgt)
- Bed fordringshaveren om at kontrollere deres firewall (porten der bruges er ikke standard, derfor er den ofte lukket) og åbne op for porten hvis nødvendigt.
- Kontrollere at de kalder med korrekt certifikat (men der burde man få en anden fejl, da browseren har spurgt efter hvilket certifikat man vil bruge)

[™] SSL/TLS padding fejl

I forbindelse med KOBRAs restance-kørsel, blev der set forskellige SSL/TLS fejl i KOBRAs ende, eksempelvis:

Log-fejl

```
2019-08-13 21:19:21,696 WARN [[STUCK] ExecuteThread: '4' for queue:
'weblogic.kernel.Default (self-tuning)'] logging.LogUtils (LogUtils.java:443)
- Interceptor for {http://www.springframework.org/schema/beans}MFKvi
tteringHentServiceSynkronPortTypeImplService#{http://skat.dk/begrebsmodel/200
9/01/15/}getMFKvitteringHent has thrown exception, unwinding now
org.apache.cxf.interceptor.Fault: Connection has been shutdown:
javax.net.ssl.SSLException: Invalid TLS padding data
        at.
org.apache.cxf.interceptor.LoggingInInterceptor.logging(LoggingInInterceptor.
java:167)
        at
org.apache.cxf.interceptor.LoggingInInterceptor.handleMessage(LoggingInInterc
eptor.java:78)
        at.
org.apache.cxf.phase.PhaseInterceptorChain.doIntercept(PhaseInterceptorChain.
java:262)
        at org.apache.cxf.endpoint.ClientImpl.onMessage(ClientImpl.java:800)
```



at org.apache.cxf.transport.http.HTTPConduit\$WrappedOutputStream.handleResponseI nternal(HTTPConduit.java:1694) at. org.apache.cxf.transport.http.HTTPConduit\$WrappedOutputStream.handleResponse(HTTPConduit.java:1530) at org.apache.cxf.transport.http.HTTPConduit\$WrappedOutputStream.close(HTTPCondu it.java:1438) at org.apache.cxf.io.CacheAndWriteOutputStream.postClose(CacheAndWriteOutputStre am.java:50) at. org.apache.cxf.io.CachedOutputStream.close(CachedOutputStream.java:229) at. org.apache.cxf.transport.AbstractConduit.close(AbstractConduit.java:56) at. org.apache.cxf.transport.http.HTTPConduit.close(HTTPConduit.java:659)

Det viste sig, at de kunne fremtvinge fejlen, ved blive ved med at lave kvitteringhent kald på 1000 fordringer.

En ændring i Java.security i KOBRAs ende løste problemet.

Følgende post beskriver problemet:

https://stackoverflow.com/questions/40964961/intermittent-javax-net-ssl-failure-bad-record-mac/41143041

Løsningen er altså:

jdk.tls.disabledAlgorithms=SSLv3, DH, DHE, ECDH, ECDHE

En anden løsning er at opgradere fra Java 7 til Java 8.

* Client received SOAP Fault from server

This error can be due to following:

- 1. The time difference in the server at the client is big. They need to adjust the clock at their server
- 2. The encryption and decryption is not working at the client.

---[HTTP response - https://ind-b2b-mf.skat.dk:7213/services/FordringIndberetService - 500]---



null: HTTP/1.1 500 Server Error

Content-Length: 424

Content-Type: application/soap+xml; charset=UTF-8

Date: Tue, 25 Aug 2020 10:57:35 GMT

Server: Jetty(9.2.15.v20160210)

<soap:Envelope xmlns:soap="<u>http://www.w3.org/2003/05/soap-</u> envelope"><soap:Body><soap:Fault><soap:Code><soap:Value>soap:Sender</soap:Value><soa p:Subcode><soap:Value xmlns:ns1="<u>http://ws.apache.org/wss4j</u>">ns1:SecurityError</soap:Value></soap:Subcode></soa p:Code><soap:Reason><soap:Text xml:lang="en">A security error was encountered when verifying the message</soap:Text></soap:Reason></soap:Fault></soap:Body></soap:Envelope>------

[WSGW] Something went wrong!

<u>com.sun.xml.internal.ws</u>.fault.ServerSOAPFaultException: Client received SOAP Fault from server: A security error was encountered when verifying the message Please see the server log to find more detail regarding exact cause of the failure.

at

com.sun.xml.internal.ws.fault.SOAP12Fault.getProtocolException(SOAP12Fault.java:214)

at

com.sun.xml.internal.ws.fault.SOAPFaultBuilder.createException(SOAPFaultBuilder.java:116)

at

com.sun.xml.internal.ws.client.sei.StubHandler.readResponse(StubHandler.java:238)

at

<u>com.sun.xml.internal.ws</u>.db.DatabindingImpl.deserializeResponse(DatabindingImpl.java:189)

at

<u>com.sun.xml.internal.ws</u>.db.DatabindingImpl.deserializeResponse(DatabindingImpl.java:276)

at

com.sun.xml.internal.ws.client.sei.SyncMethodHandler.invoke(SyncMethodHandler.java:104)



at

com.sun.xml.internal.ws.client.sei.SyncMethodHandler.invoke(SyncMethodHandler.java:77)

at <u>com.sun.xml.internal.ws</u>.client.sei.SEIStub.invoke(SEIStub.java:147)

at com.sun.proxy.\$Proxy39.getMFFordringIndberet(Unknown Source)

at

com. supeo. wsgw. WSGWC lient Handler. handle Fordring Indberet (WSGWC lient Handler. java: 153)

at com.supeo.wsgw.WSGWClientHandler.run(WSGWClientHandler.java:86)

at java.lang.Thread.run(Thread.java:745)

Java tip: Slå full debugging til

Java Tip

Kør dit program med:

-<u>Djavax.net</u>.debug=all