Nye sertifikat

Veilder/ FAQ

Konsulentavdelingen DIPS Front
13.06.2025
Distribusjon: DIPS Begrenset

DIPS Front
Trollhaugmyra 15
5353 Straume
Norway
dips.no/front
+47 75 59 20 00

Innhold

1 Om veilederen 1

2 Bistand i fra DIPS Front 1

3 Sertifikatenes plassering 1

4 Virksomhetssertifikat 1

4.1 Digihelse 1

4.2 KPR innsendingsprogram 2

4.3 E-meldinger 3

Virksomhetssertifikat for lokal partner 3

4.4 Authentication 6

4.5 SkatteIntegrasjonAPI 6

5 SSL sertifikat 7

5.1 Internet Information Services (IIS) 7

5.2 Authentication 10

5.3 NGINX container for SvarUT 11

5.3.1 Felles 11

5.3.2 For kunder med en installasjon 11

5.3.3 For kunder med samdrift 11

5.3.4 Felles 12

5.3.5 For kunder med en installasjon 12

5.3.6 For kunder med samdrift 12

1 Om veilederen

Denne veilederen har til hensikt å gi deg en oversikt over hva som må utføres ved bytte av virksomhetssertifikat og ved bytte av SSL sertifikat, i forhold til CosDoc.

Virksomhetssertifikatet benyttes av:

1. Digihelse
2. KPR
3. E-meldinger – (DIPS Communicator og i NHN adresseregister)
4. «Authentication»- (brukes av Persontjenesten, Kjernejournal, SvarUT)
5. Skatt (KS integrasjon)

SSL sertifikatet benyttes av

- Alle CosDoc sine tjenester i IIS (Internet Information Services)
- «Authentication»- (brukes av Persontjenesten, Kjernejournal, SvarUT).
- NGINX container – på Linux server som kjører SvarUT

2 Bistand i fra DIPS Front

Dersom dere har behov for bistand til oppdatering av sertifikat, kan dette meldes inn via support.dips.no, kategori «Bestilling», prioritet «konsulent», så vil en av våre tekniske konsulenter bistå dere. Bistand faktureres etter medgått tid og gjeldende timesatser.

3 Sertifikatenes plassering

Sertifikatene importeres inn i sertifikatlager på applikasjonsserver.
De skal ligge under lokal maskin -> personlig.

4 Virksomhetssertifikat

Sertifikater for virksomheten må skaffes fra en offentlig godkjent sertifikattilbyder, som for eksempel BuyPass.

DIPS Front kan bistå med bestilling og installasjon hvis dette er ønskelig. Kunde bestiller da bistand via support.dips.no med kategori «Bestilling – annet».

Virksomhetssertifikatet består av to deler: autentiseringssertifikat og tilhørende privat nøkkel, samt signeringssertifikat og tilhørende privat nøkkel. Privatnøkkelen er beskyttet av passord.

4.1 Digihelse

Det er to filer som må oppdateres ved nytt virksomhetssertifikat.

1. Åpne «services.msc» på CosDoc applikasjonsserver og finn de to Windows tjenestene som starter på «Digihelse».

2. Åpne egenskapene og se hvor disse tjenestene ligger. Det er en «appsettings.json» for hver av de to tjenestene, i hver sin mappe.

3. Inne i «appsettings.json», for hver av tjenestene, finnes det en seksjon som heter «CertSettings». Her finnes det «EncryptionThumbprint» og «SigningThumbprint». Det er verdiene bak disse som skal oppdateres.

4. Verdiene finner man ved å åpne egenskapene for sertifikatet og finne Thumbprint (eller Avtrykk på norsk), evt. så kan det også hentes ut ved hjelp av f.eks. powershell.

   Hvis OS er eldre enn Windows Server 2019 vær obs på at man gjerne får med ekstra tegn når thumbprint kopieres. Pass på at det ikke er noen ekstra tegn med!

   Sertifikatet med «Key Usage» «Non-Repudation» brukes som Signing.
   Sertifikatet med «Key Usage» «Digital Signature, Key Encipherment, Data Encipherment» brukes som Encryption.

5. Gi servicebruker som kjører de to Digihelsetjenestene, lesetilgang til sertifikatenes privatnøkkel.

6. Restart tjenestene etter at "appsettings.json" er oppdatert.

4.2 KPR innsendingsprogram

Det er to filer for KPR innsendingsprogrammet, som må oppdateres ved nytt virksomhetssertifikat.

1. Åpne «services.msc» på CosDoc applikasjonsserver og finn de to Windows tjenestene som starter på «KPR».

2. Åpne egenskapene og se hvor disse tjenestene ligger. Det er en «appsettings.json» for hver av de to tjenestene, i hver sin mappe.

3. Inne i «appsettings.json», for hver av tjenestene, finnes det en seksjon som heter «CertSettings». Her finnes det «EncryptionThumbprint» og «SigningThumbprint». Det er verdiene bak disse som skal oppdateres.

4. Verdiene finner man ved å åpne egenskapene for sertifikatet og finne Thumbprint (eller Avtrykk på norsk), evt. så kan det også hentes ut ved hjelp av f.eks. powershell.

   Hvis OS er eldre enn Windows Server 2019 vær obs på at man gjerne får med ekstra tegn når thumbprint kopieres. Pass på at det ikke er noen ekstra tegn med!

   Sertifikatet med «Key Usage» «Non-Repudation» brukes som Signing.
   Sertifikatet med «Key Usage» «Digital Signature, Key Encipherment, Data Encipherment» brukes som Encryption.

5. Gi servicebruker som kjører de to Digihelsetjenestene, lesetilgang til sertifikatenes privatnøkkel.

6. Restart tjenestene etter at «appsettings.json» er oppdatert.

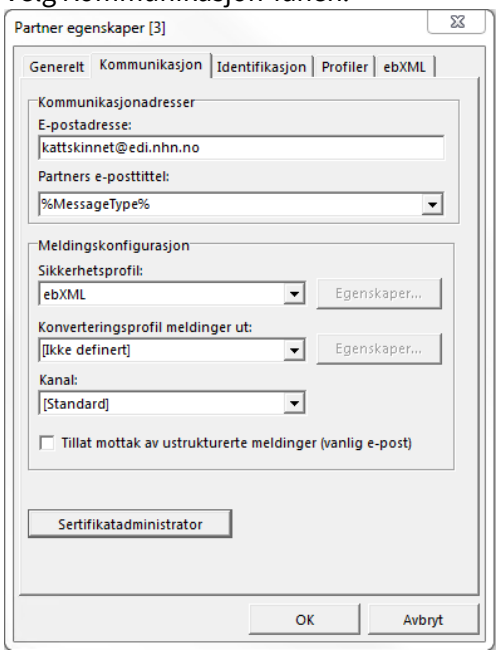
4.3 E-meldinger

Virksomhetssertifikatene som skal benyttes for meldingsutveksling må lastes opp i NHN adresseregister. Ta kontakt med NHN adresseregister ved spørsmål om dette.

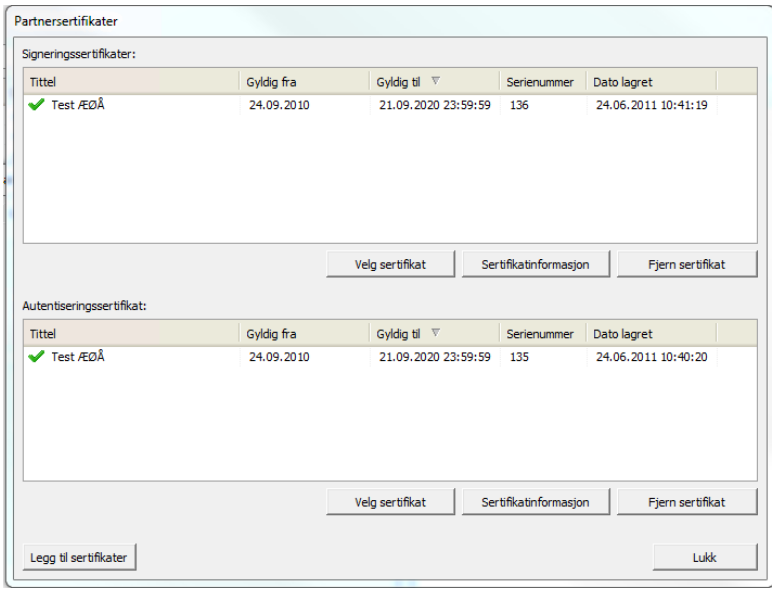
Følgende veiledning er hentet fra brukerdokumentasjonen for DIPS Communicator:

Virksomhetssertifikat for lokal partner

1. Velg lokal partner i partnerlista.
2. Dobbelt klikk på partneren og dialogen Partner egenskaper kommer opp.
3. Velg Kommunikasjon-fanen.

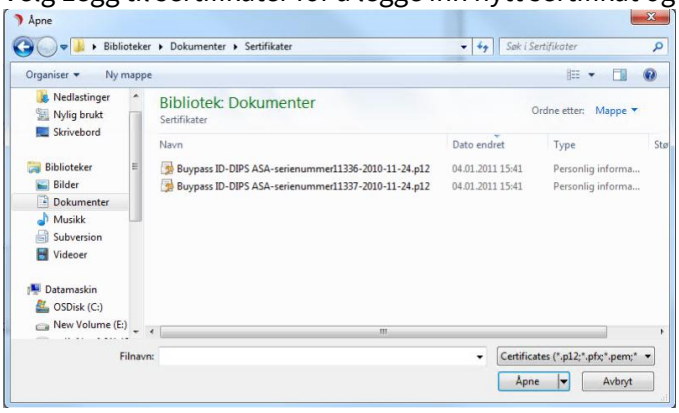


4. Trykk Sertifikatadministrator-knappen for å åpne sertifikat-komponenten i DIPS Communicator:



Fra dialogen Partnersertifikater kan sertifikater inspiseres, legges til og slettes. Over tid vil sertifikatenes gyldighetsperiode gå ut, og nye bli lagt til.

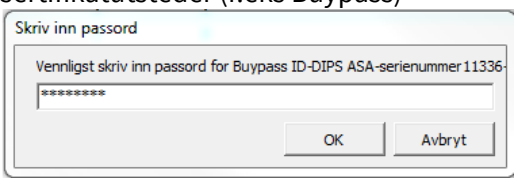
5. Velg Legg til sertifikater for å legge inn nytt sertifikat og tilhørende privat nøkkel:



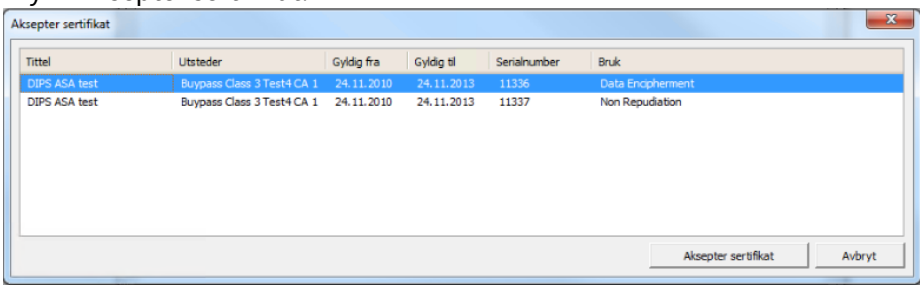
Sertifikater lastes inn fra filsystem.

6. Velg de(n) aktuelle filen(e) i filsystem-dialogen for å laste inn fra filsystem ved å bla i kataloger og disker som normalt.

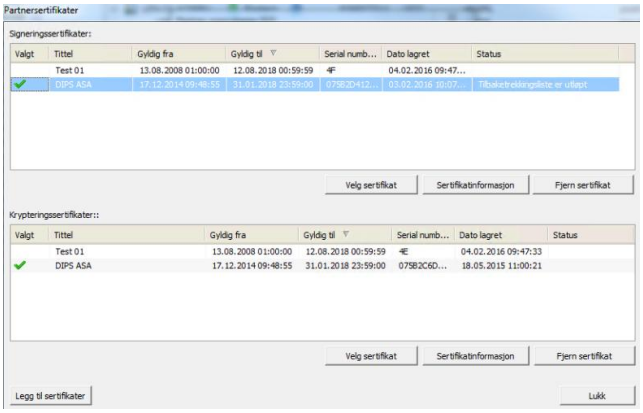
7. Du blir nå bedt om å legge inn passord for sertifikatet. Passordet utstedes av sertifikatutsteder (f.eks Buypass)



8. Trykk Aksepter sertifikat:



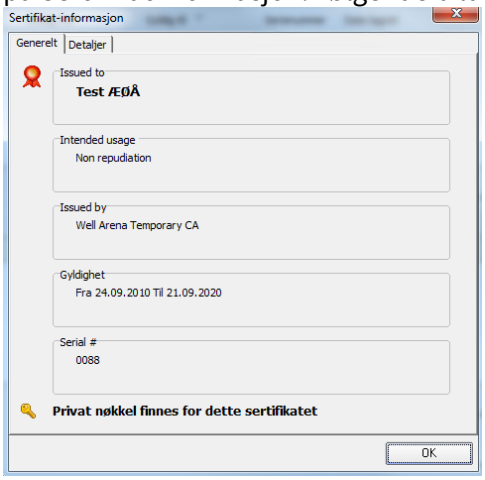
9. De nye sertifikatene vil nå være lagt til i listene over signerings- og autentiseringssertifikater. Sjekk Status-feltet for informasjon.



10. Merk riktig signeringssertifikat i lista og trykk Velg sertifikat. Dette sertifikatet vil da bli validert og valgt ved signering av meldinger. Hvis man ikke velger, eller valgt sertifikatet er ugyldig vil DIPS Communicator automatisk velge det eldste gyldige sertifikatet ved neste meldingsutveksling.

11. Merk riktig autentiseringssertifikat i lista og trykk Velg sertifikat. Dette sertifikatet vil da bli validert og valgt ved kryptering av meldinger. Hvis man ikke velger, eller valgt sertifikatet er ugyldig vil DIPS Communicator automatisk velge det eldste gyldige sertifikatet ved neste meldingsutveksling.

12. Sjekk sertifikatet ved å merke det sertifikatet du ønsker å se på og trykke på Sertifikatinformasjon. Følgende bilde kommer opp:



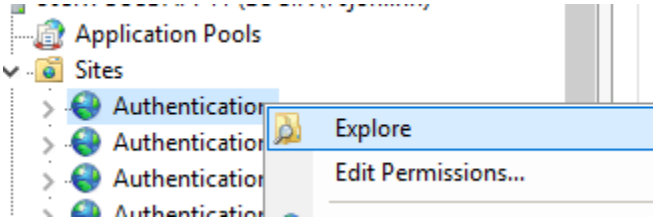
Kontroller at sertifikatet er identisk med forventet sertifikat, gjerne ved å sammenlikne serienummer, gyldighetsdatoer og og 'Utstedt til'-informasjon med informasjon fra utsteder.

4.4 Authentication

Authentication er en Web-tjeneste som brukes av flere andre tjenester, for å autentisere pålogget bruker.

1. Åpne Internet Information Services (IIS) Manager

2. Under «Sites», finn «Authentication» for Drift, og åpne installasjonsmappen ved å høyreklikke og velge «explore».



3. Åpne «appsettings.json», og finn «ClientCertThumbprint» og «SigningCertificateThumbprint». Det er verdiene bak disse som skal oppdateres.
4. For SigningCertificateThumbprint brukes sertifikatet med «Key Usage» «Non-Repudation».

   For ClientCertThumbprint brukes sertifikatet med «Key Usage» «Digital Signature, Key Encipherment, Data Encipherment».

   Verdiene finner man ved å åpne egenskapene for sertifikatet og finne Thumbprint (eller Avtrykk på norsk), evt. så kan det også hentes ut ved hjelp av f.eks. powershell.

   Hvis OS er eldre enn Windows Server 2019 vær obs på at man gjerne får med ekstra tegn når thumbprint kopieres. Pass på at det ikke er noen ekstra tegn med!

5. Åpne applicationpool tilhørende Authentication, og sjekk at servicebruker har leserettigheter til sertifikatets privatnøkkel.

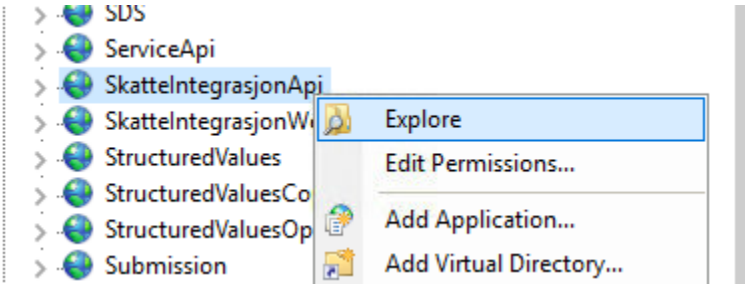
6. Recycle applicationpool for authentication.

4.5 SkatteIntegrasjonAPI

Skatteintegrasjonsløsningen som skal ivareta innhenting av likningsopplysninger, bruker også virksomhetssertifikat. Løsningen bruker kun signeringssertifikatet.

1. Åpne Internet Information Services (IIS) Manager

2. Under «Sites», finn «SkatteIntegrasjonApi» fo, og åpne installasjonsmappen ved å høyreklikke og velge «explore».



3. Inne i «appsettings.json», finnes det en seksjon som heter «MaskinportenConfig». Her finner du «SertifikatAvtrykk». Det er verdiene bak denne som skal oppdateres.

4. Sertifikatet som benyttes er det med "Key Usage" "Non-Repudation".

   Verdien finner man ved å åpne egenskapene for sertifikatet og finne Thumbprint (eller Avtrykk på norsk), evt. så kan det også hentes ut ved hjelp av f.eks. powershell.

   Hvis OS er eldre enn Windows Server 2019 vær obs på at man gjerne får med ekstra tegn når thumbprint kopieres. Pass på at det ikke er noen ekstra tegn med!

5. Åpne applicationpool tilhørende «SkatteIntegrasjonApi», og sjekk at servicebruker har leserettigheter til sertifikatets privatnøkkel.

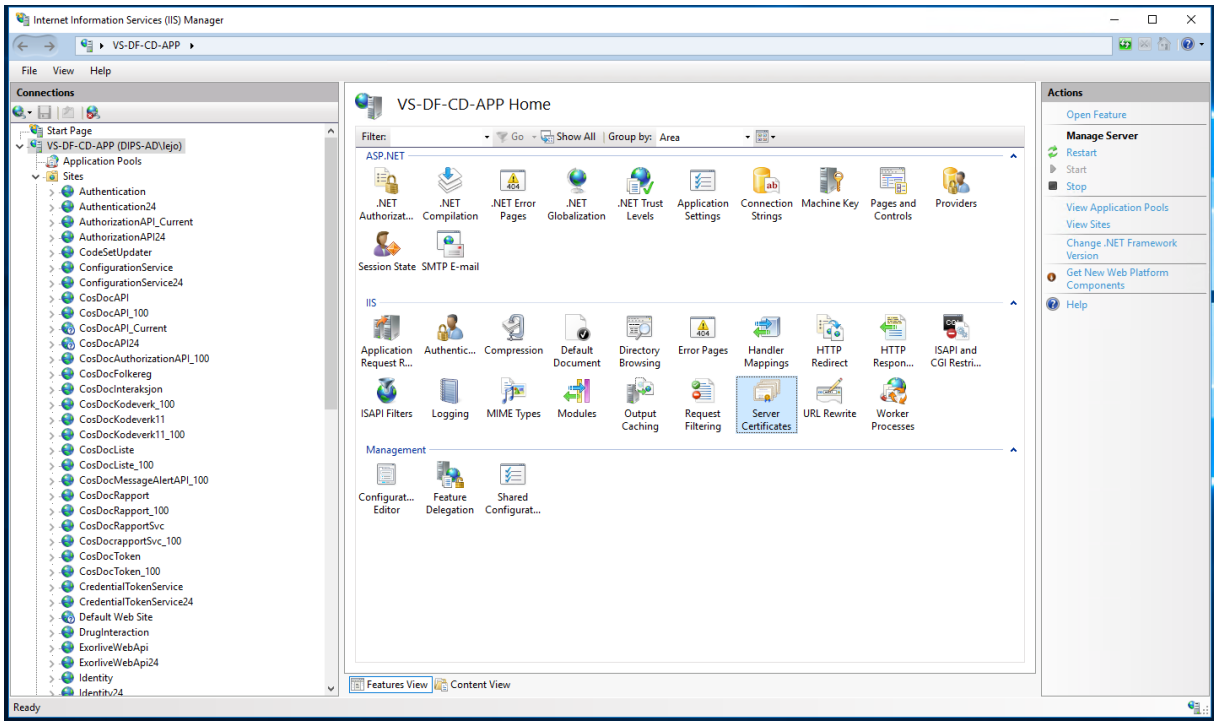
6. Recycle applicationpool for SkatteIntegrasjonApi.

5 SSL sertifikat

5.1 Internet Information Services (IIS)

Det er viktig at Lokal IT avdeling har kontroll på SSL sertifikatets utløpsdato.

Dette kan man enkelt finne i IIS under «Server Certificates».

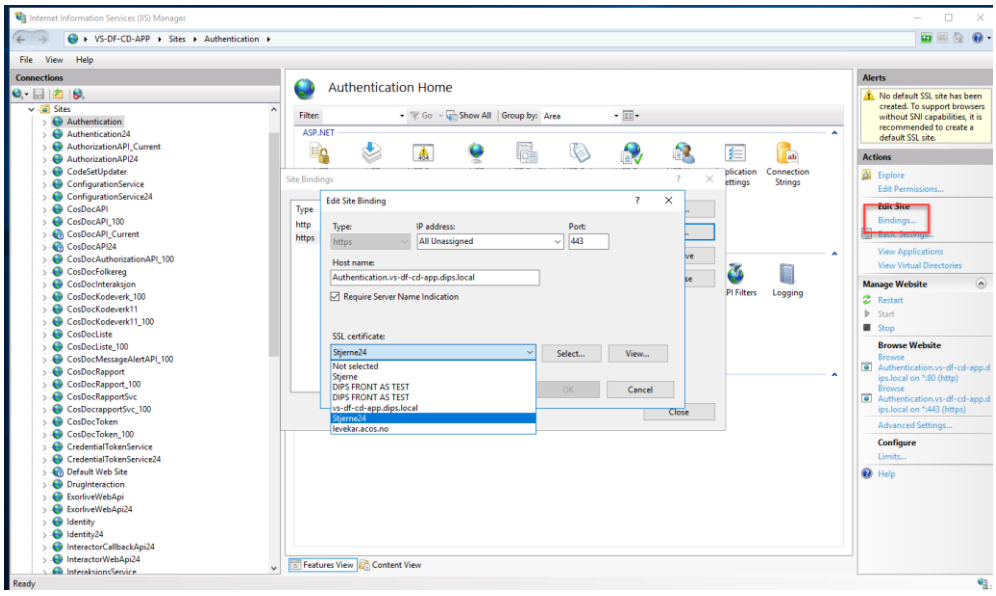


Alle tjenestene må ha et gyldig SSL sertifikat.

Når utløpsdatoen for det gamle SSL sertifikatet nærmer seg, må organisasjonen;

1. Legge inn et nytt SSL sertifikat på server (se punkt 2)

2. Velge det nye SSL sertifikatet for tjenestene i IIS

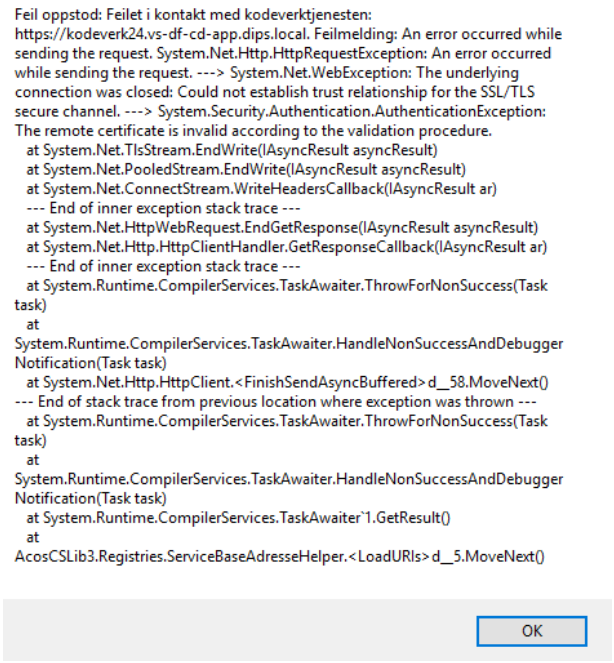


Dersom SSL sertifikatet utløper uten å bli oppdatert, vil dette føre til at ansatte ikke får logget på CosDoc.

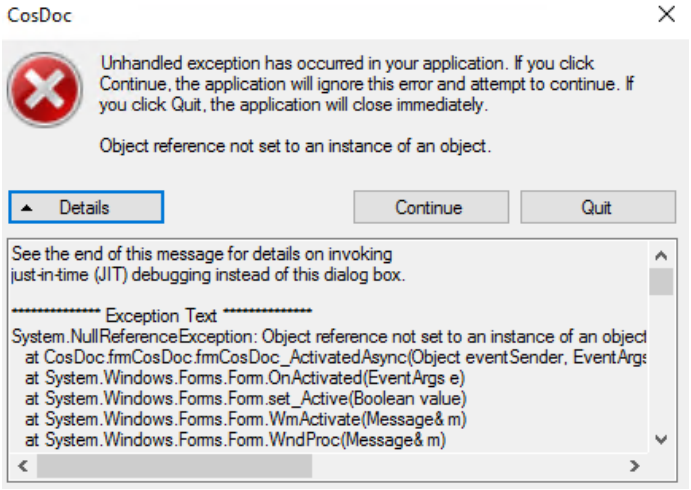
IT avdelingen bør alltid sjekke SSL sertifikatets gyldighet før feilmeldinger ved pålogging til CosDoc meldes til DIPS Front support.

Se eksempel på feilmeldinger hvor «kodeverk»-tjenesten har et utløpt SSL sertifikat:

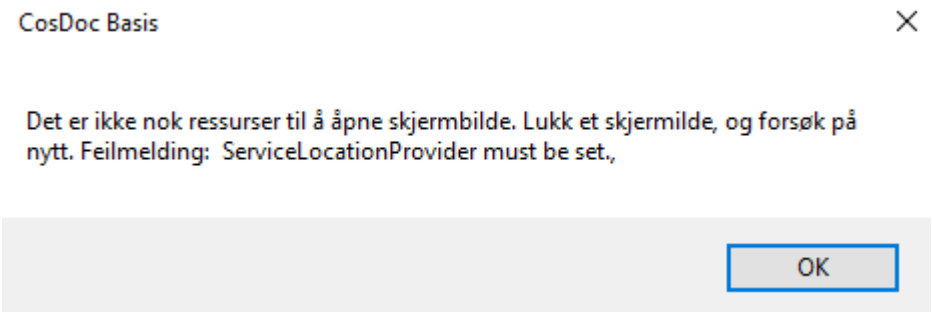
1.



2.



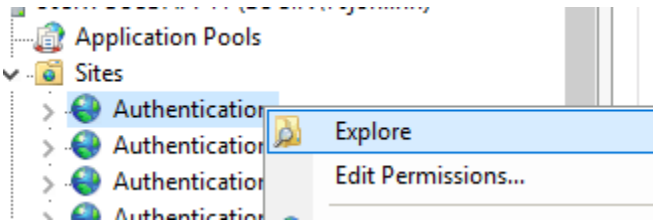
3.



5.2 Authentication

Authentication er en Web-tjeneste som brukes av flere andre tjenester, for å autentisere pålogget bruker. Denne tjenesten bruker SSL sertifikatet.

1. Åpne Internet Information Services (IIS) Manager
2. Under «Sites», finn «Authentication» for Drift, og åpne installasjonsmappen ved å høyreklikke og velge «explore».



3. Åpne «appsettings.json», og finn «SSLCertificateThumbprint». Det er verdien bak denne som skal oppdateres.

4. Verdien finner man ved å åpne egenskapene for SSL sertifikatet og finne Thumbprint (eller Avtrykk på norsk), evt. så kan det også hentes ut ved hjelp av f.eks. powershell.

   Hvis OS er eldre enn Windows Server 2019, vær obs på at man gjerne får med ekstra tegn når thumbprint kopieres. Pass på at det ikke er noen ekstra tegn med!

5. Åpne applicationpool tilhørende «Authentication», og sjekk at servicebruker har leserettigheter til sertifikatets privatnøkkel.

6. Recycle applicationpool for authentication.

5.3 NGINX container for SvarUT

Ved bytte av SSL-sertifikatet som benyttes for SvarUt, må de nye sertifikatfilene legges tilgjengelig på Linux-serveren og gjøres tilgjengelige for NGINX-containeren. Denne veiledningen dekker installasjonen hos de fleste kunder, men det kan forekomme avvik – verifiser derfor gjerne stier før arbeidet påbegynnes.

Merk: Dersom det benyttes et annet utstedende sertifikat, må filen med sertifikatkjeden også byttes. Dette omfattes ikke av denne veiledningen.

I denne veilederen brukes 'samdrift' om installasjoner der det kjøres flere SvarUt-installasjoner på én Linux-server

5.3.1 Felles

1. Få tak i nytt sertifikat i PFX format, sikre at du har passordet.
2. Overfør denne til Linux-server med SCP eller PSCP
3. Eksempel kode (sti til sertifikatfil, linuxuser og IP må rettes):

   scp C:\path\to\cert.pfx linuxuser@192.168.1.100:/home/linuxuser/

4. Bruk openssl til å konvertere sertifikat til to filer:
   openssl pkcs12 -in /home/linuxuser/cert.pfx -clcerts -nokeys -out /home/linuxuser/cert.crt
   openssl pkcs12 -in /home/linuxuser/cert.pfx -nocerts -nodes -out /home/linuxuser/cert.rsa

5.3.2 For kunder med en installasjon

5. Kopier/Flytt sertifikatfilene til /usr/containers/svarut/persistent/

Eksempel:

cp /home/linuxuser/cert.crt /usr/containers/svarut/persistent/cert.crt
cp /home/linuxuser/cert.rsa /usr/containers/svarut/persistent/cert.rsa

6. Åpne /usr/containers/svarut/prod.env for redigering:
   Sudo nano /usr/containers/svarut/prod.env

5.3.3 For kunder med samdrift

5. Kopier/Flytt sertifikatfilene til /usr/containers/nginx/persistent/
   Eksempel:
   cp /home/linuxuser/cert.crt /usr/containers/nginx/persistent/cert.crt

cp /home/linuxuser/cert.rsa /usr/containers/nginx/persistent/cert.rsa

6. Åpne /usr/containers/nginx/persistent/prod.env for redigering:
   Sudo nano /usr/containers/nginx/persistent/prod.env

5.3.4 Felles

7. Endre filnavn for sertifikatene i prod.env
   SSL_CERT_FILENAME = cert.crt
   SSL_CERT_KEY_FILENAME = cert.rsa

5.3.5 For kunder med en installasjon

8. Start på nytt, naviger til */usr/containers/svarut/*
   Sudo docker compose --env-file prod.env down
   Sudo docker compose --env-file prod.env up -d

5.3.6 For kunder med samdrift

8. Start på nytt, naviger til /usr/containers/nginx/
   Sudo docker compose --env-file prod.env down
   Sudo docker compose --env-file prod.env up -d