Nye sertifikat

Veilder/ FAQ

Konsulentavdelingen DIPS Front
19.02.2024
Distribusjon: DIPS Begrenset

ENABLING EFFICIENT HEALTHCARE

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

Innhold

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:

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

SSL sertifikatet benyttes av

- «Authentication»- (brukes av Persontjenesten, Kjernejournal, SvarUT)

2 Sertifikatenes plassering

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

3 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.

3.1 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.

3.2 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.

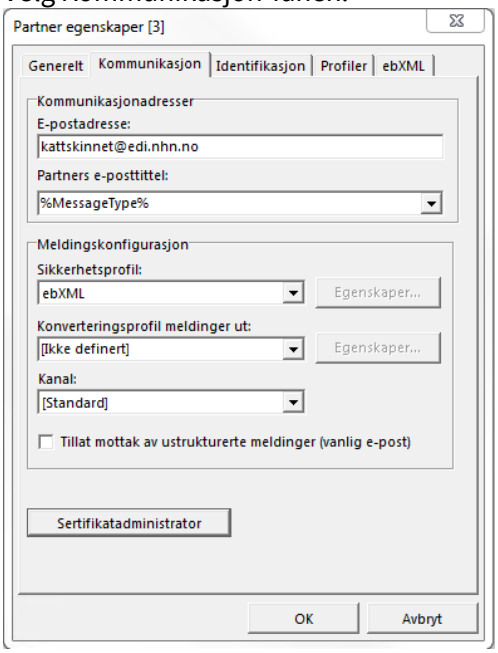
3.2 E-meldinger

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

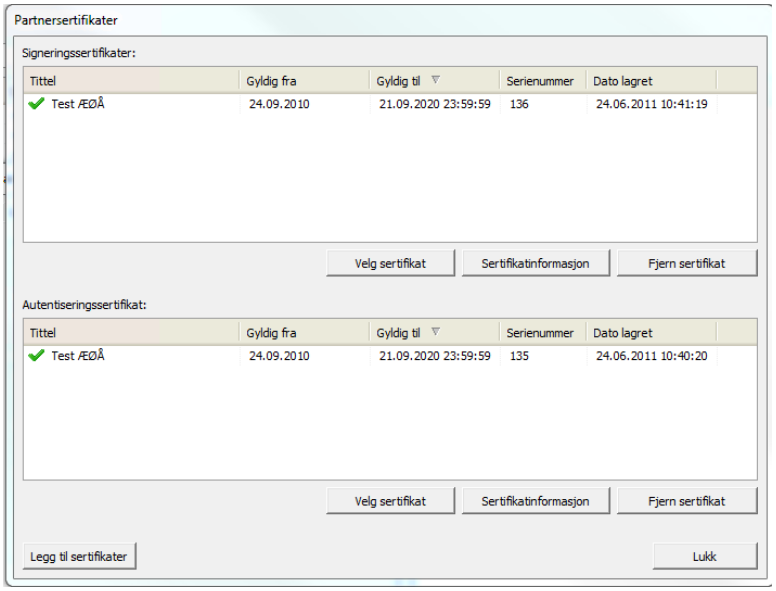
Følgende veiledning er hentet fra brukerdokumentasjonen for DIPS Communicator:

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.

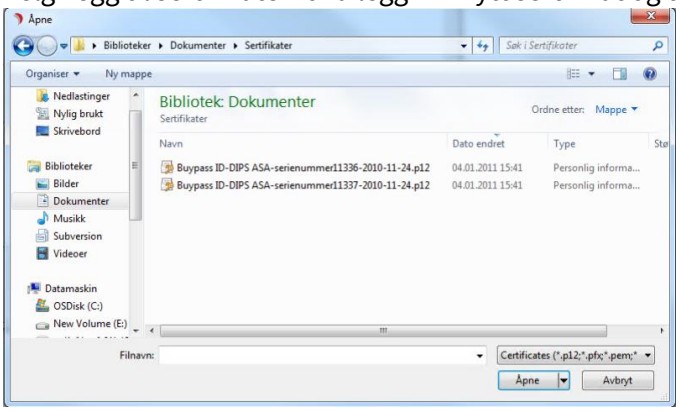


4. Trykk Sertifikatadministrator-knappen for å åpne sertifikat-komponenten i DIPS Communicator:



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

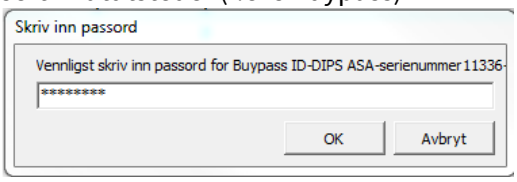
5. Velg Legg til sertifikater for å legg inn nytt sertifikat og tilhørende privat nøkkel:



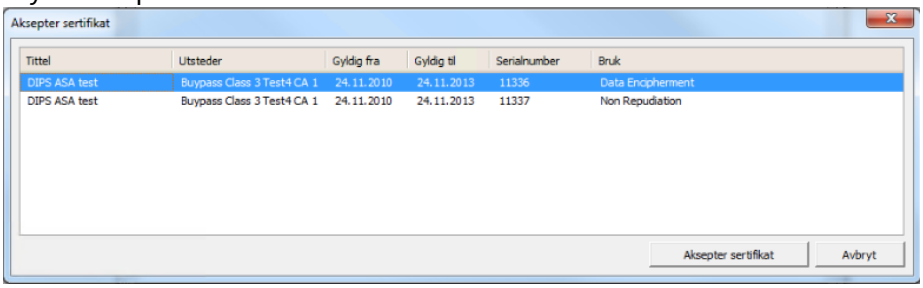
Sertifikater lastes inn fra filsystem.

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.

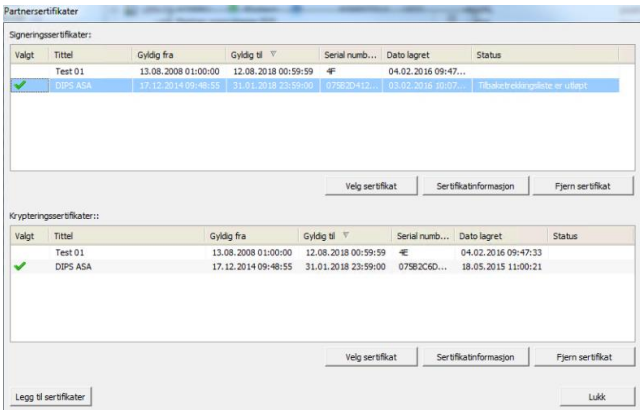
7. Du blir nå bedt om å legge inn passord for sertifikatet. Passordet utstedes av sertifikatutsteder (f.eks Buypass)



8. Trykk Aksepter sertifikat:



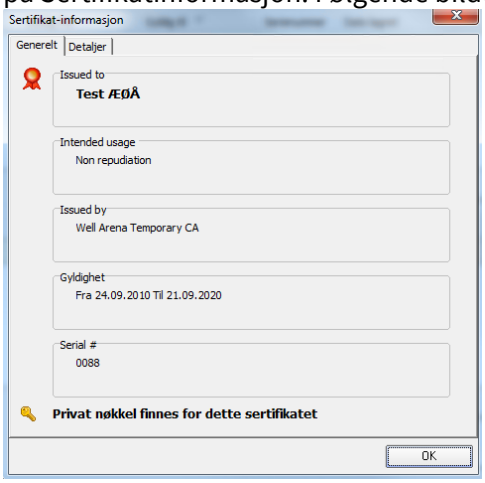
9. De nye sertifikatene vil nå være lagt til i listene over signerings- og autentiseringssertifikater. Sjekk Status-feltet for informasjon.



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:



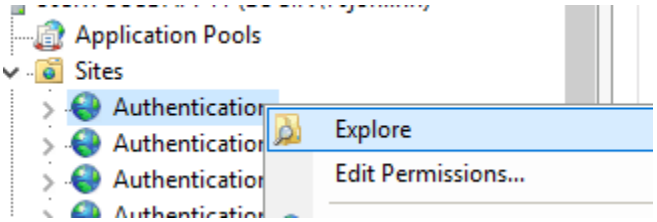
Kontroller at sertifikatet er identisk med forventet sertifikat, gjerne ved å sammenlikne serienummer, gyldighetsdatoer og og 'Utstedt til'-informasjon med informasjon fra utsteder.

3.3 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!

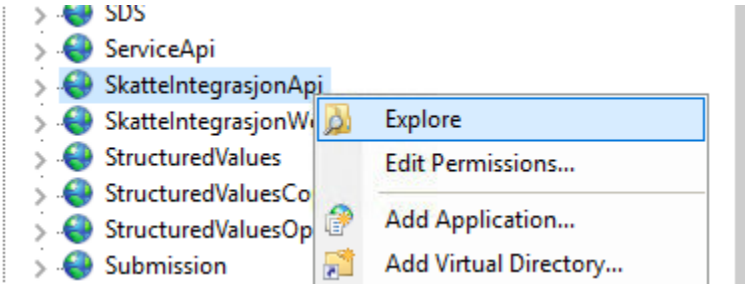
5. Åpne applicationpool tilhørende Authentication, og sjekk at servicebruker har leserettigheter til sertifikatets privatnøkkel.

6. Recycle applicationpool for authentication.

3.4 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.

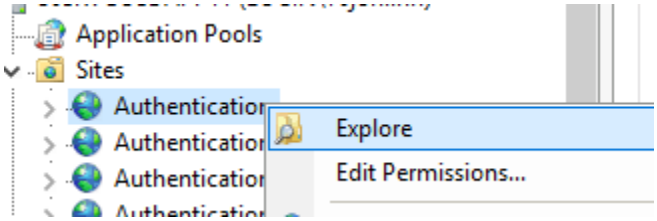
6. Recycle applicationpool for SkatteIntegrasjonApi.

4 SSL sertifikat

4.1 Authentication

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

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



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

10. 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!

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

12. Recycle applicationpool for authentication.