FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Internet Information Server 7.0/7.5 SSL certifikat administration

Følgende vejledning beskriver hvordan man installerer et certifikat på en IIS 7.0-7.5 server.

For support og hjælp til anvendelsen af denne vejledning kan du kontakte FairSSL på e-mail info@fairssl.dk eller telefon +45 77 345 678. For certifikat bestilling, certifikat sammenligning og flere vejledninger se websitet på www.fairssl.dk.

Hvis serveren er tilgængelig fra internettet bør installationen efterfølgende testes gratis på www.fairssl.dk/ssltest/

Indholdsfortegnelse

VIGTIG INFORMATION – LÆS MIG!

Genstart af server og / eller services kan være nødvendige, inden ændringerne fra vejledningen kan ses.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

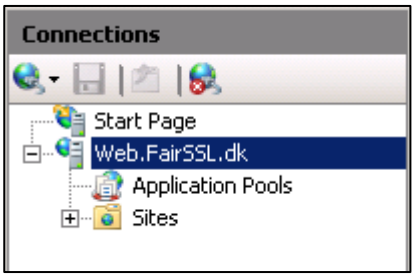
Generering af CSR til certifikat bestilling

Følgende beskriver hvordan certificate signing request (CSR) genereres på en Microsoft IIS 7.

1. Log ind på serveren med en konto der er medlem af gruppen ”Administrators” på den lokale server.

2. Under ”Administrative Tools” startes ” Internet Information Services (IIS) Manager”.

3. Vælg webserveren.



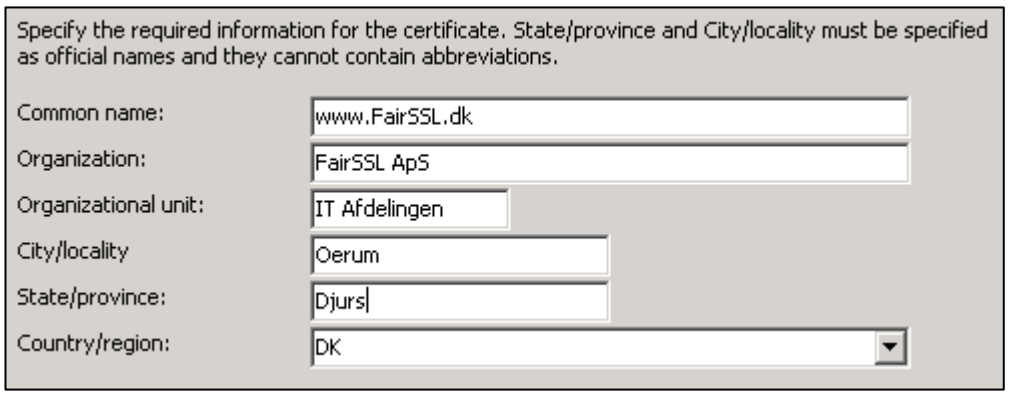
4. Vælg ”Server Certificates”.

5. Under ”Actions” vælges ”Create Certificate Request”.

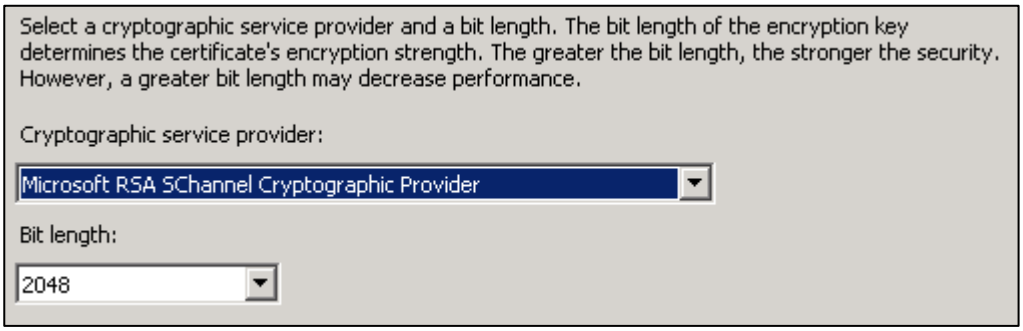
6. Indtast oplysninger for certificatet som sendes til udstederen. Alle indtastninger vist her er for FairSSL som et eksempel og skal tilrettes så det passer jeres organisation. For at være sikker på at certifikatet kan udstedes uden problemer bør ”ÆØÅ” og andre specialtegn undlades.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

7. Navn på certifikatet og virksomheds oplysninger.



8. Vælg kryptering, **mindst 2048 Bit.**



9. Vælg en placering til CSR filen.

10. Der er nu oprettet en CSR som kan bruges til certifikat bestillingen.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Import af mellemudsteder certifikat ("Intermediate Certificate Authority")

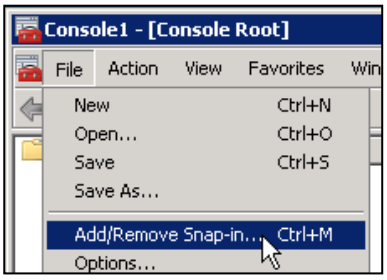
Følgende beskriver hvordan mellemudsteder certifikater installeres på en Microsoft Windows baseret server og derved også en SBS 2003 server. For at sikre at klienter kan godkende mellemudstedere i certifikatet, skal certifikatets mellemudstederes offentlige certifikat installeres på SBS 2003 serveren. Ved modtagelse af et GlobalSign certifikat, vil du også modtage de offentlige certifikater for mellemudstederne.

1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.

2. Kopier teksten med mellemudsteder certifikatet ("Intermediate certificate"), fra e-mailen med dit nye certifikat, til en simpel tekst editor (som Notepad). Gem filen på skrivebordet, med filnavnet "mellemudsteder.cer".

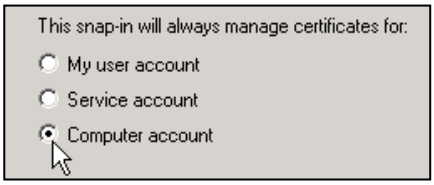
3. Skriv følgende kommando "mmc.exe".

4. Vælg "Add/Remove Snap In".



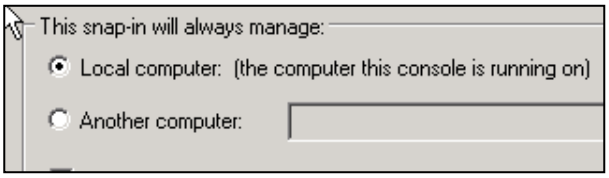
5. Vælg "Certificates" og tryk "Add"

6. Vælg "Computer account"



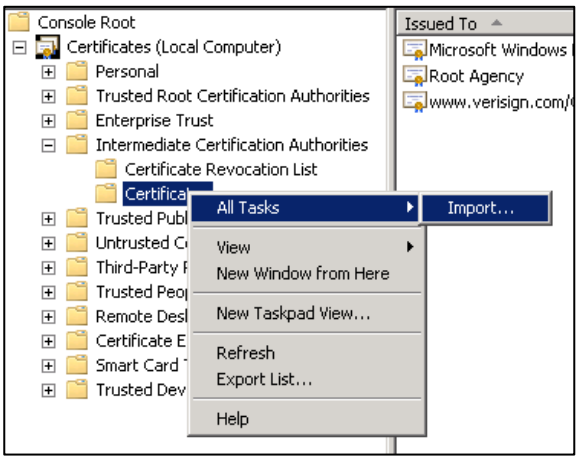
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

7. Vælg ”Local computer”

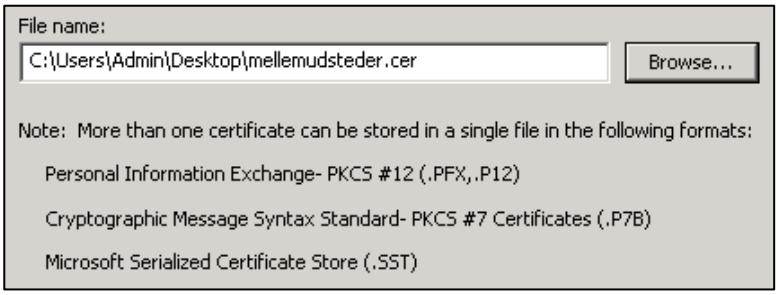


8. Under “Certificates (Local Computer)” udvid “Intermediate Certification Authorities” og “Certificates”.

9. Højre klik på ”Certificates” og vælg ”All-Tasks” og ”Import”.



10. Vælg filen som tidligere blev gemt på skrivebordet.



11. Kontrollere at certifikatet bliver gemt i ”Intermediate Certification Authorities”

12. Mellemudsteder certifikatet er nu importeret.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Afslutning af afventende certifikat request

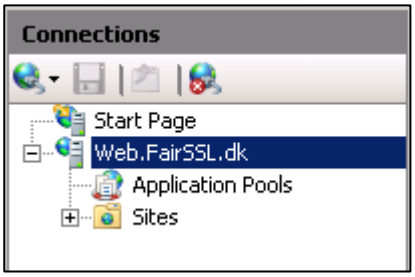
Følgende beskriver hvordan et certifikat installeres, efter at være udstedt fra en CSR der er genereret på denne server tidligere.

1. Log ind på serveren med en konto der er medlem af gruppen ”Administrators” på den lokale server.

2. Kopier teksten med certifikatet, fra e-mailen med dit nye certifikat, til en simpel tekst editor (som Notepad). Gem filen på skrivebordet med et passende filnavn, og en endelse på ”.cer” eller ”.pem”. I eksemplet her er filnavnet ”www.FairSSL.dk.cer”

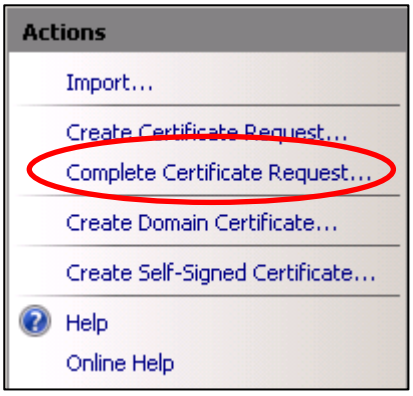
3. Under ”Administrative Tools” startes ”Internet Information Services (IIS) Manager”

4. Vælg webserveren.



5. Vælg ”Server Certificates”.

6. Under ”Actions” vælges ”Complete Certificate Request”.

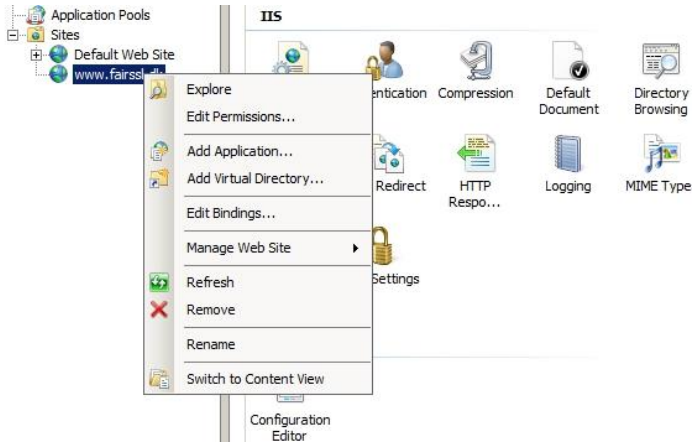


FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

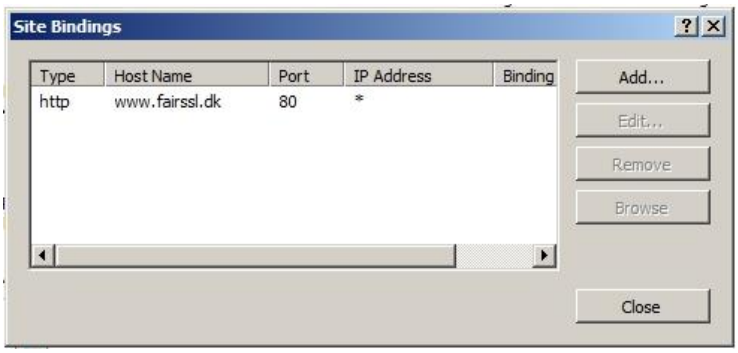
7. Vælg filen som tidligere blev gemt på skrivebordet, og vælg et kaldenavn for certifikatet.

8. Certifikatet er nu installeret på serveren, men det er endnu ikke tilføjet til et website.

9. Højreklik på websitet og vælg ”Edit Bindings...”



10. I Site Bindings, Klik på knappen ”Add…”

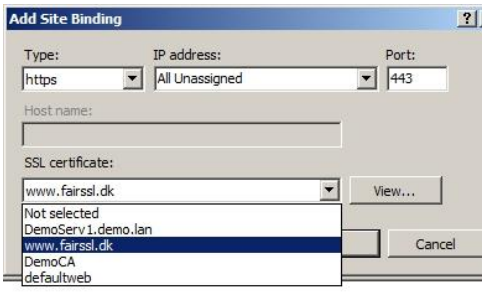


11.

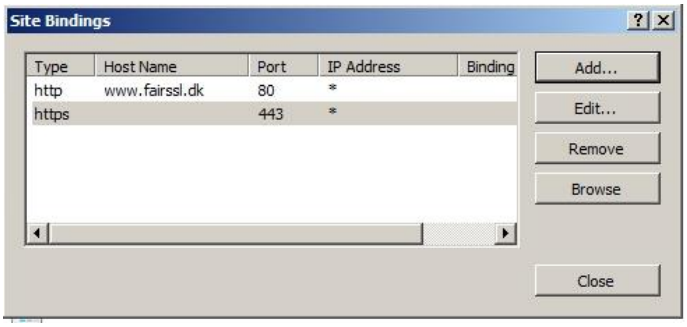
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

12. Vælg HTTPS som type

13. Vælg det ønskede certifikat og klik på OK knappen



14. Klik på Close – knappen for at lukke vinduet med Site Bindings



Certifikatet er nu aktiveret for det valgte website.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Import af certifikat fra certifikat backupfil (.PFX)

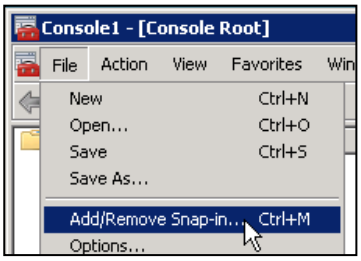
Følgende beskriver hvordan installere et certifikat fra en .pfx fil.
Ved bestilling af domæner med FairCSR modtages certifikatet som en backup fil, beskyttet med en unik kode.

1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.

2. Gem den modtagne fil på skrivebordet.

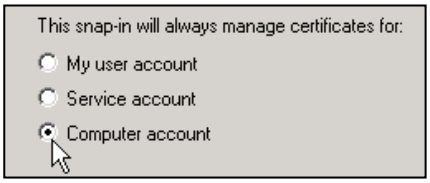
3. Skriv følgende kommando "mmc.exe".

4. Vælg "Add/Remove Snap In".

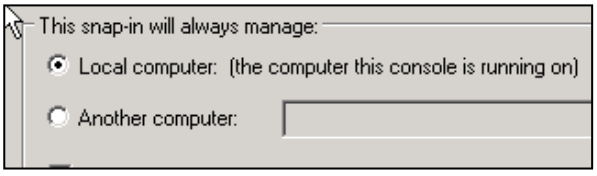


5. Vælg "Certificates" og tryk "Add"

6. Vælg "Computer account"



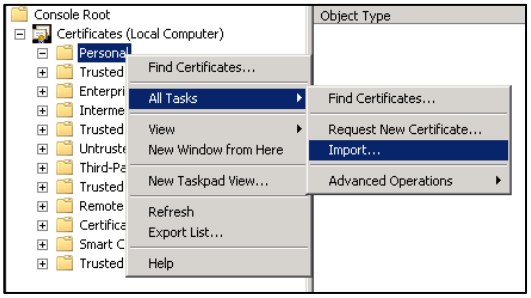
7. Vælg "Local computer"



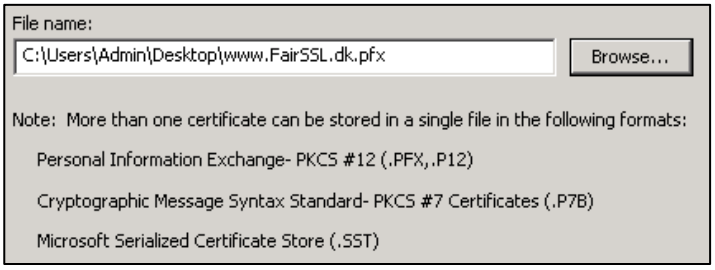
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

8. Under “Certificates (Local Computer)” udvid “Personal”

9. Højre klik på ”Personal” og vælg ”All-Tasks” og ”Import”.



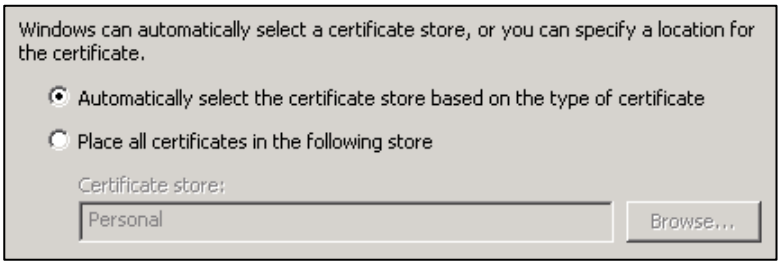
10. Vælg filen som tidligere blev gemt på skrivebordet.



11. Indtast den kode certifikatet er krypteret med. Denne kode er modtaget på SMS.

Bemærk: Hvis du senere vil kunne eksportere certifikatet til en ny backupfil, skal der være et hak i ”Mark this key as exportable”.

12. Vælg ”Automatically select the certificate store based on the type of certificate”.



FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

13. Certifikatet er nu importeret.

Opsætning af installeret certifikat på website

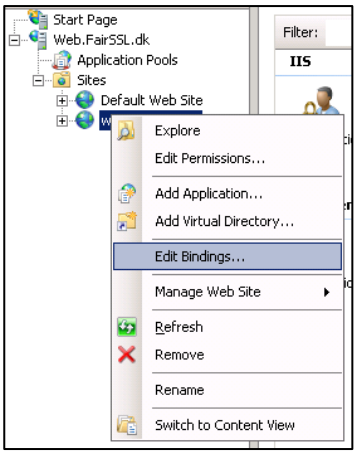
Følgende beskriver hvordan et allerede installeret certifikat tilknyttes et website.

1. Log ind på serveren med en konto der er medlem af gruppen ”Administrators” på den lokale server.

2. Under ”Administrative Tools” startes ”Internet Information Services (IIS) Manager”

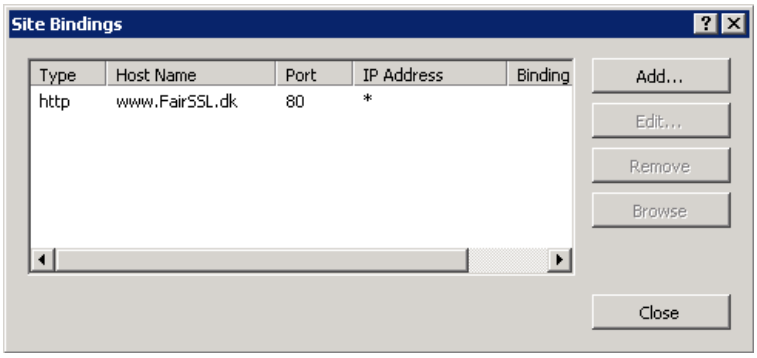
3. Udvid ”Sites”.

4. Højre klik på det ønskede website, og vælg egenskaber (”Edit Bindings”).

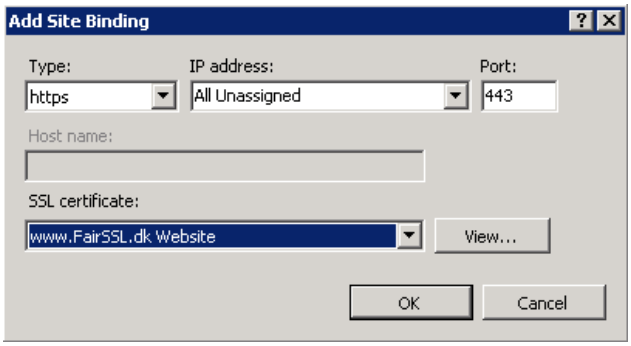


FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

5. Vælg ”Add”.



6. Vælg ”HTTPS” som type, IP adressen, port og certifikat.



7. Certifikatet er nu aktiveret på websitet.

8. Test at certifikatet virker korrekt på https://www.fairssl.dk/ssltest/.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Fornyelse af certifikater

Certifikater har en begrænset levetid. Dette betyder at de med tiden skal fornyes for fortsat at virke.
En fornyelse af et certifikat kan ske på 2 måder:

- Som om at det er et helt nyt certifikat.
  Teknisk set er der tale om et helt nyt certifikat som intet har at gøre med det gamle.

- Det eksisterende certifikat opdateres med ny udløbsdato og serienummer.
  Teknisk set beholdes den private nøgle og det offentlige del af certifikatet overskrives med nye informationer.

NB: I begge tilfælde skal man være opmærksom på at serienummeret på det gamle certifikat bliver listet som invalidt – også selv om at det gamle certifikat endnu ikke er løbet ud.
Alle steder hvor certifikatet er installeret, skal det derfor opdateres (f.eks. webserver/mailserver/firewalls).

Start fornyelse af eksisterende certifikat med CSR

NB! Når du på denne måde fornyer et eksisterende certifikat, påvirkes det certifikat som allerede er installeret. Den private nøgle i certifikatet bliver genbrugt, men den offentlige del af certifikatet bliver overskrevet med et nyt certifikat som har samme navn men ny udløbsdato og nyt serienummer.

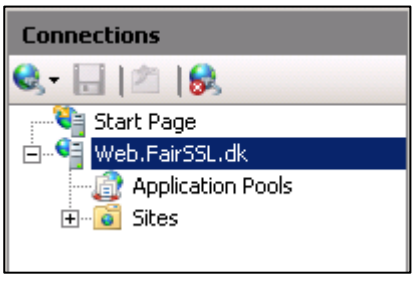
Hvis du vil undgå at ændre i det eksisterende certifikat, skal du gøre som ved bestilling af et komplet nyt certifikat. Se guiden Generering af CSR til certifikat bestilling

Følgende beskriver hvordan et certifikat fornyes på og der genereres en CSR til bestilling.

1. Log ind på serveren med en konto der er medlem af gruppen ”Administrators” på den lokale server.

2. Under ”Administrative Tools” startes ” Internet Information Services (IIS) Manager”.

3. Vælg webserveren.

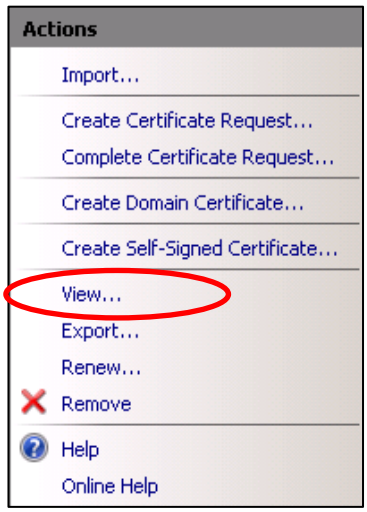


FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

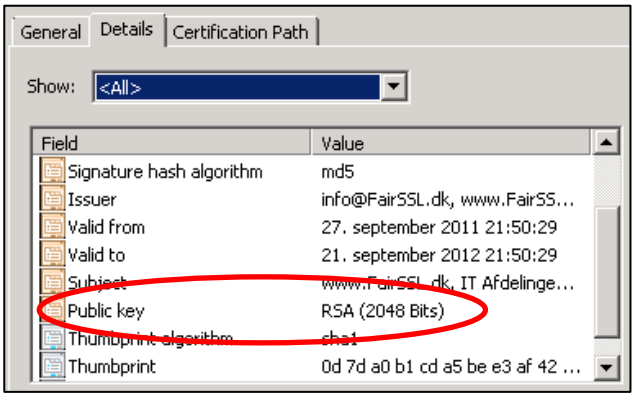
4. Vælg ”Server Certificates”.

5. Marker det certifikat der skal fornyes.

6. Under ”Actions” vælg ”View”

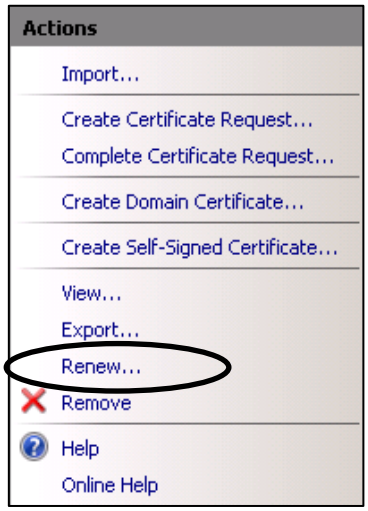


7. På fanebladet ”Details” findes ”Public key”. Hvis certifikatet er udstedt med ”RSA (2048 Bits)” fortsættes guiden. **Er certifikatet udstedt med ”RSA (1024 Bits)” eller mindre, afsluttes denne guide, og guiden ”Generering af CSR til certifikat bestilling” startes for at lave en ny bestilling.**

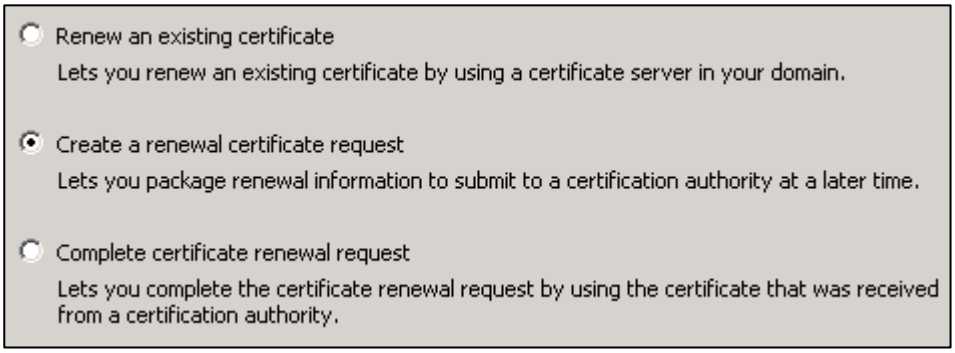


FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

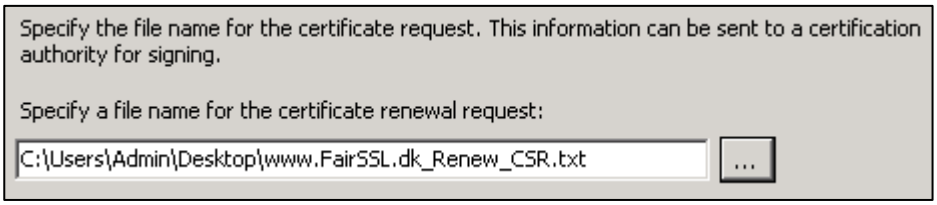
8. Under ”Actions” vælg ”Renew”.



9. Vælg ”Create a renewal certificate request”.



10. Vælg en placering til din CSR fil.



11. Der er nu oprettet en CSR som kan bruges til certifikat bestillingen.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Afslut fornyelse af certifikat med CSR

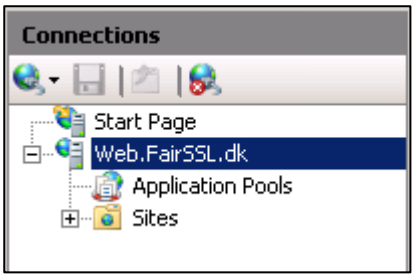
Følgende beskriver hvordan certifikat fornyelsen afsluttes.

1. Log ind på serveren med en konto der er medlem af gruppen ”Administrators” på den lokale server.

2. Kopier teksten med certifikatet, fra e-mailen med dit nye certifikat, til en simpel tekst editor (som Notepad). Gem filen på skrivebordet med et passende filnavn, og en endelse på ”.cer” eller ”.pem”. I eksemplet her er filnavnet ”www.FairSSL.dk_Renew.cer”.

3. Under ”Administrative Tools” startes ” Internet Information Services (IIS) Manager”.

4. Vælg webserveren.

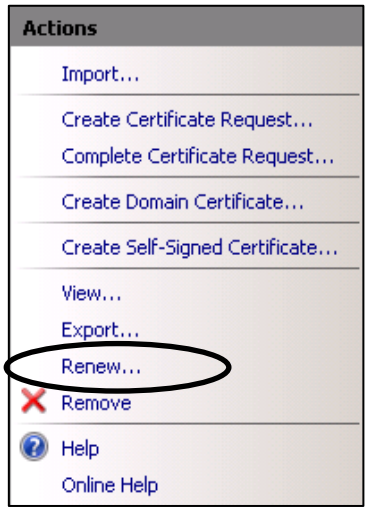


5. Vælg ”Server Certificates”.

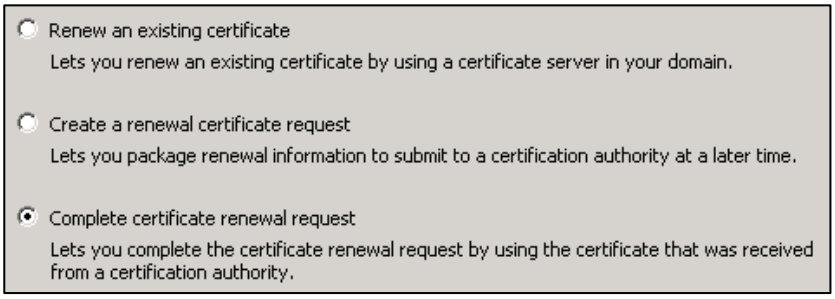
6. Marker det certifikat som du er i gang med at forny.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

7. Under ”Actions” vælg ”View”



8. Vælg ”Complete certificate renewal request”.



9. Vælg filen som tidligere blev gemt på skrivebordet, og klik på Finish-knappen.

10. Certifikatet er nu installeret og klar til brug.

Nyt certifikat eller fornyelse af certifikat

På denne måde kan du både oprette helt nye certifikater samt få fornyet eksisterende certifikater uden at ødelægge/ændre det eksisterende.
Hvis du fornyer et eksisterende certifikat på denne måde, vil du til slut have både et gammelt og et nyt certifikat som du kan vælge imellem.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Gå ind i IIS manaageren