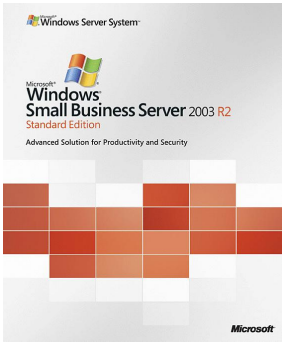
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Small Business Server 2003 Certifikat administration

Følgende vejledning beskriver hvordan man vælger hvilke adresser der skal være i ens SBS 2003 SSL certifikat.



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

Husk at teste din installation når du er færdig 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.

Version 1.0 – september 2011

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

Valg af certifikat

Til en simpel opsætning af en SBS 2003 server, hvor der kun anvendes Outlook Web Acces og Remote Web Workplace. Her kan med fordel bruges et certifikat uden SAN option bruges.

Hvis SharePoint anvendes kan der være en fordel i at vælge et certifikat med SAN option. Nedenstående er et eksempel på hvilke navne vi anbefaler der skal være i certifikatet

- Companyweb (Anvendes af sharepoint)
- Servernavn
- Servernavn.Domænenavn

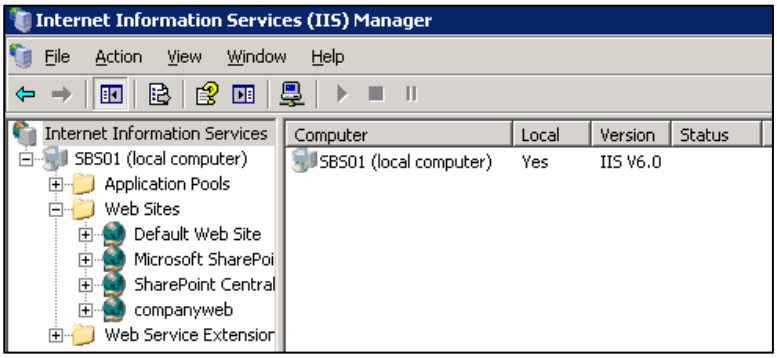
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Generering af CSR til certifikat bestilling

Følgende beskriver hvordan certificate signing request (CSR) genereres på en Microsoft SBS 2003.

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”



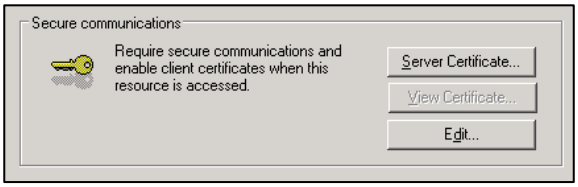
3. Højre klik på det ønskede website (”Default Web Site”), og vælg egenskaber (”Properties”).

   Bemærk ønsker du ikke at påvirke dette websites eksisterende SSL certifikat, bør du først udføre ”Fejl! Henvisningskilde ikke fundet.” sektionen af denne vejledning.

4. Vælg fanebladet ”Directory Security”.

4. Vælg fanebladet ”Directory Security”.

5. Vælg ”Server Certificate”.

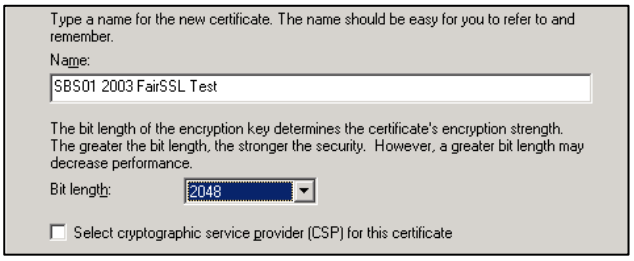


6. Herefter starter en certifikatguide. Vælg ”Create a new certificate”.

7. Vælg ”Prepare the request now, but send it later”.

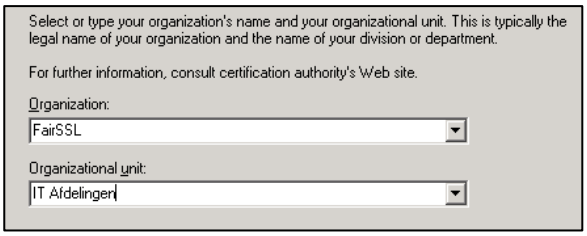
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

8. Der vælges et passende navn til certifikatet, og "Bit length" ændres til **mindst 2048.**

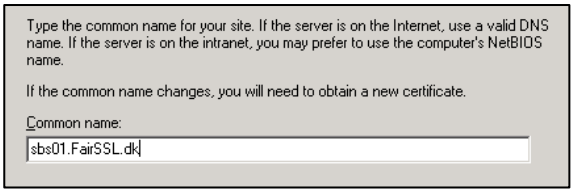


9. Indtast oplysninger for certifikatet som sendes til udstederen. Alle indtastninger vist her er for FairSSL som et eksempel og skal tilrettes så det passer jeres organisation. For at være sikker på at certifikatet kan udstedes uden problemer bør "ÆØÅ" og andre specialtegn undlades.

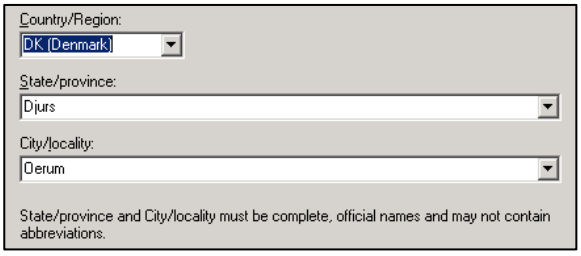
10. Indtast firmanavn og evt. afdeling.



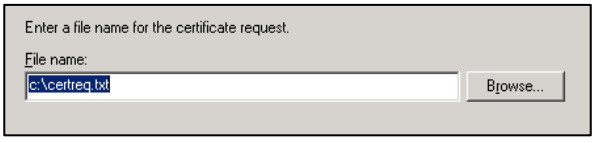
11. Navnet på det domæne certifikatet skal anvendes på.



12. Navnet på land, region og by indtastes

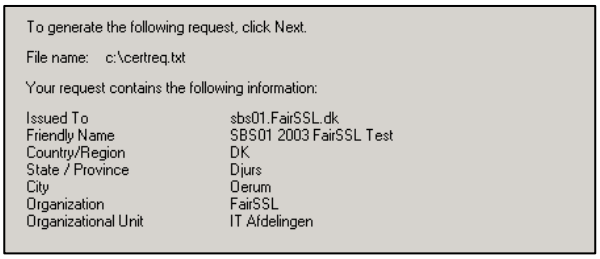


13. Vælg en placering af din CSR fil.



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

14. Overblik over indtastningerne.



15. 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

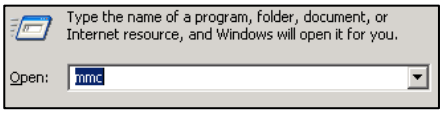
Import af mellemudsteder certifikat ("Intermediate Certificate Authority")

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.

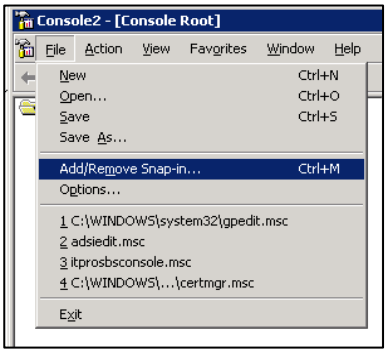
1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.

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. Vælg Start – Kør og skriv følgende kommando "mmc.exe".

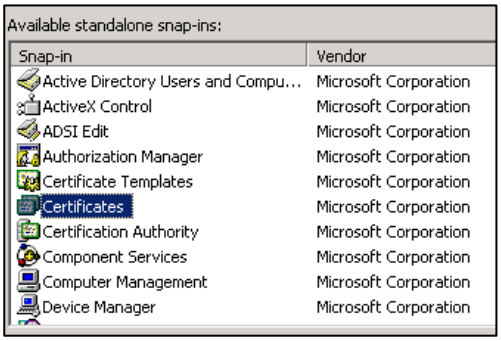


4. Vælg "Add/Remove Snap In".



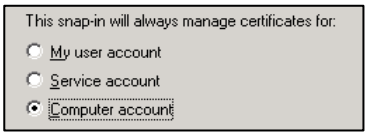
5. Vælg "Add".

6. Tilføj "Certificates".

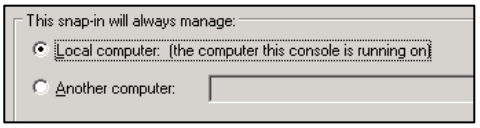


FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

7. Vælg ”Computer Account”.

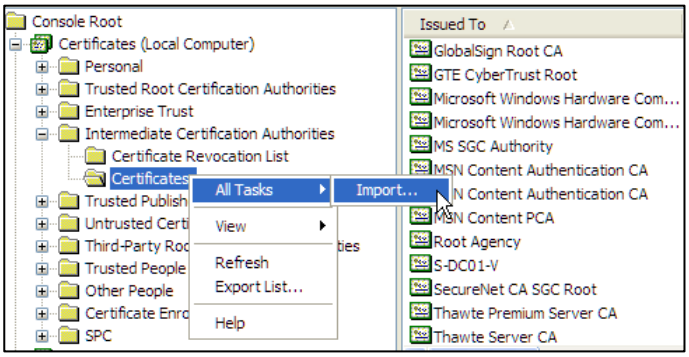


8. Vælg ”Local Computer”.

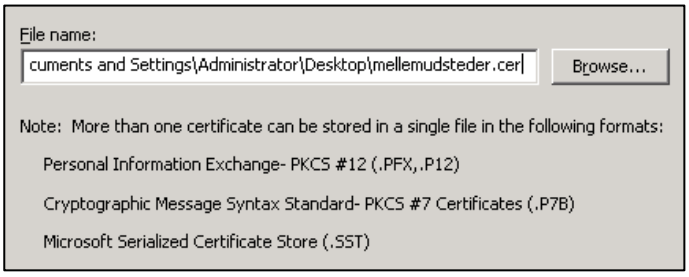


9. Under “Certificates (Local Computer)” udvid “Intermediate Certification Authorities” og “Certificates”.

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



11. Vælg filen som tidligere blev gemt på skrivebordet.



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

13. Mellemudsteder certifikatet er nu importeret.

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

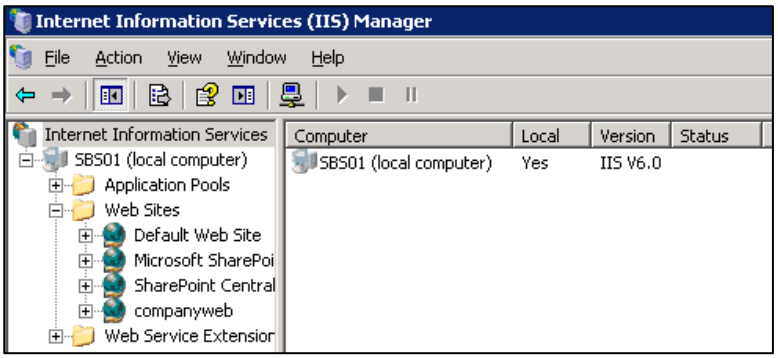
Afslutning af afventende certifikat request

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 ”SBS01-FairSSL.dk.cer”

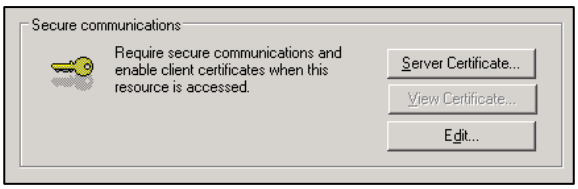
3. Under ”Administrative Tools” startes ”Internet Information Services (IIS) Manager”



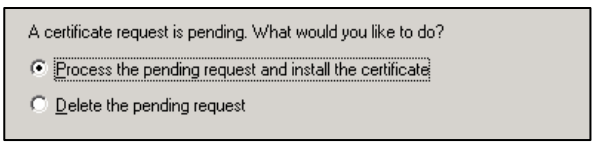
4. Højre klik på det ønskede website (”Default Web Site”), og vælg egenskaber (”Properties”).

5. Vælg fanebladet ”Directory Security”.

6. Vælg ”Server Certificate”.

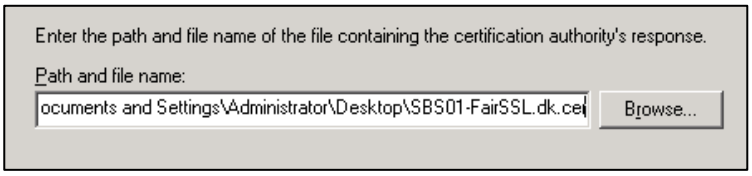


7. Herefter starter en certifikatguide. Vælg ”Process the pending request and install the certificate”.



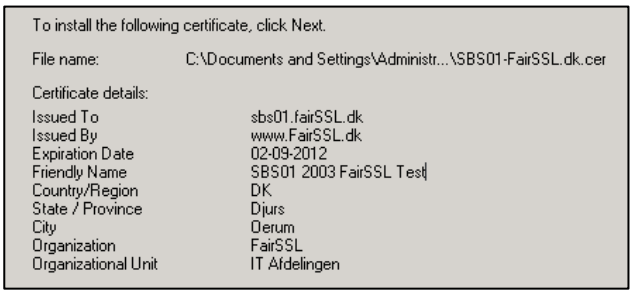
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

8. Vælg filen som tidligere blev gemt på skrivebordet.

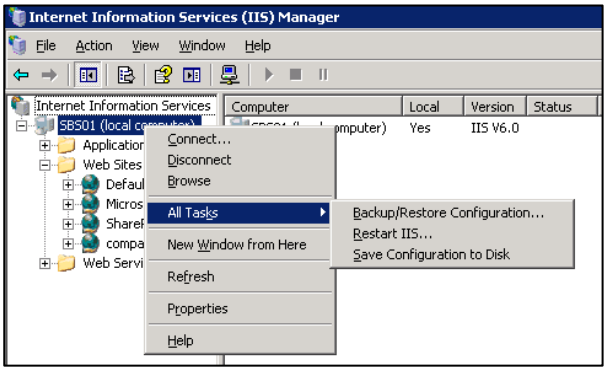


9. Vælg den port der skal bruges til HTTPS trafik, som standard benyttes port 443.

10. Overblik over det valgte certifikat.



11. højre klik på IIS serveren og vælg ”All Tasks” og dernæst ”Restart IIS…”.



12. Certifikatet er nu aktiveret på websitet.

13. 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

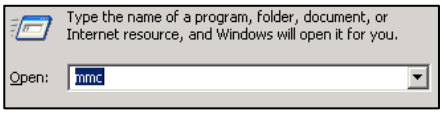
Import af certifikat udstedt med AutoCSR (.PFX)

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

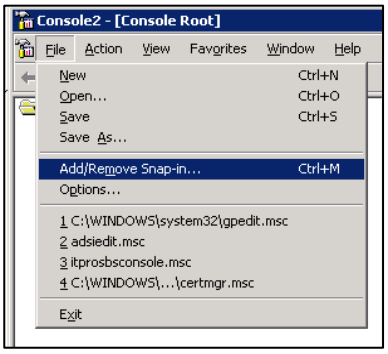
1. Log ind på serveren med en konto der er medlem af gruppen ”Administrators” på den lokale server.

2. Gem den modtagne fil på skrivebordet.

3. Vælg Start – Kør og skriv følgende kommando ”mmc.exe”.



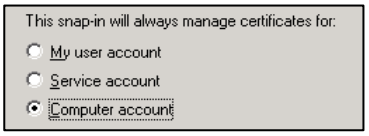
4. Vælg ”Add/Remove Snap In”.



5. Vælg ”Add”.

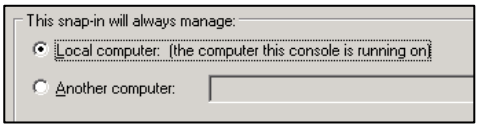
6. Tilføj ”Certificates”.

7. Vælg ”Computer Account”.



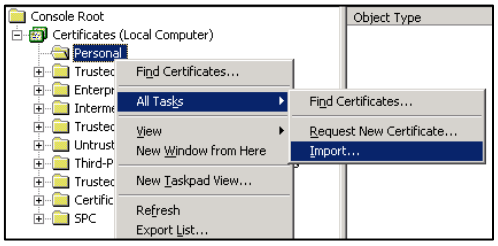
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

8. Vælg ”Local Computer”.



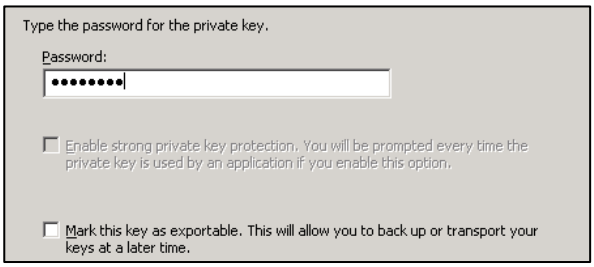
9. Under “Certificates (Local Computer)” udvid “Personal.

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

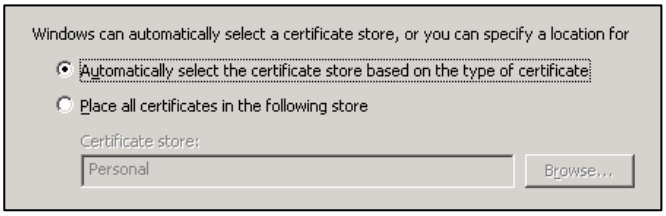


11. Vælg filen som tidligere blev gemt på skrivebordet.

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



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



14. Certifikatet er nu importeret.

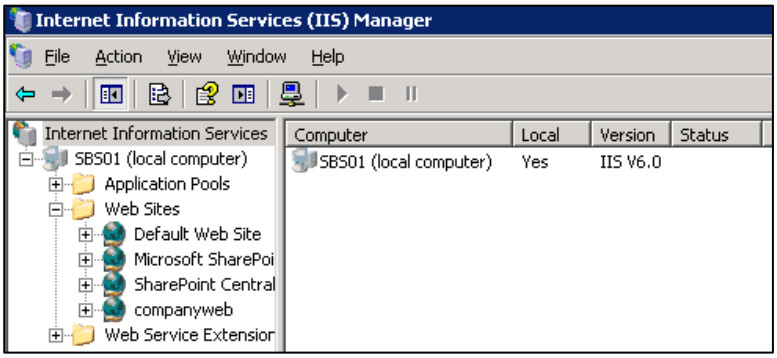
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

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.

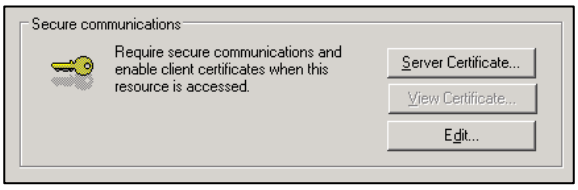
2. Under ”Administrative Tools” startes ”Internet Information Services (IIS) Manager”



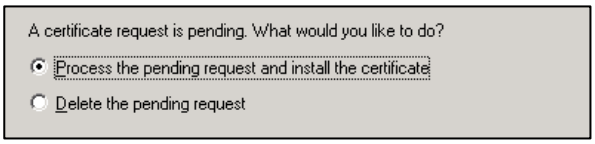
3. Højre klik på det ønskede website (”Default Web Site”), og vælg egenskaber (”Properties”).

4. Vælg fanebladet ”Directory Security”.

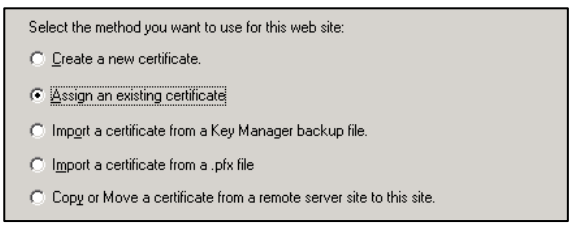
5. Vælg ”Server Certificate”.



6. Herefter starter en certifikatguide. Vælg ”Process the pending request and install the certificate”.

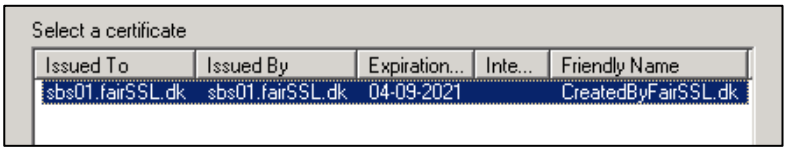


7. Vælg ”Assign an existing certificate”



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

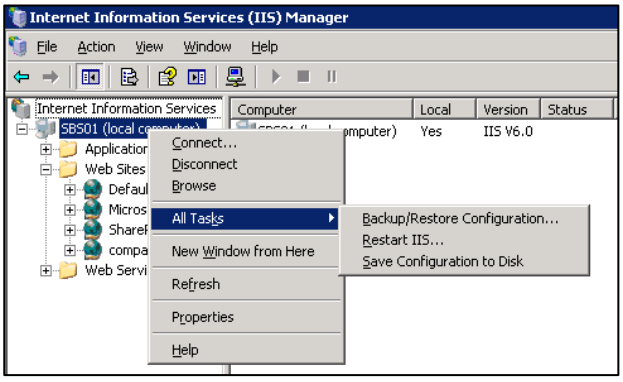
8. Vælg det certifikat der skal bruges på websitet.



9. Vælg den port der skal bruges til HTTPS trafik, som standard benyttes port 443.

10. Overblik over det valgte certifikat.

11. højre klik på IIS serveren og vælg ”All Tasks” og dernæst ”Restart IIS…”.



12. Certifikatet er nu aktiveret på websitet.

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

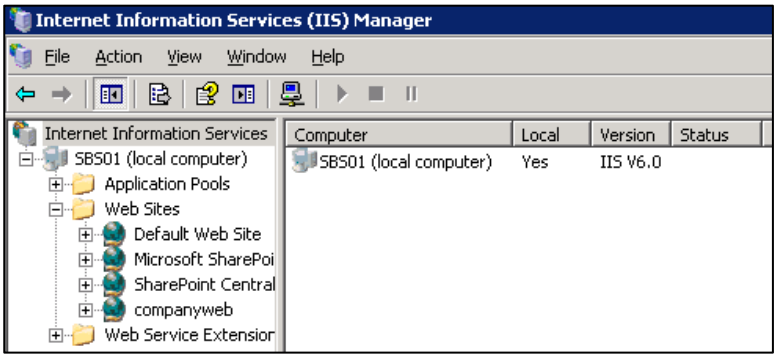
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Fornyelse af certifikat med CSR

Følgende beskriver hvordan et certifikat fornyes på et website.

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

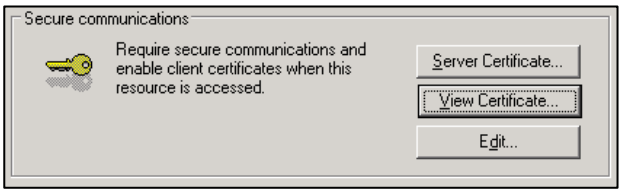
2. Under ”Administrative Tools” startes ”Internet Information Services (IIS) Manager”



3. Højre klik på det ønskede website (”Default Web Site”), og vælg egenskaber (”Properties”).

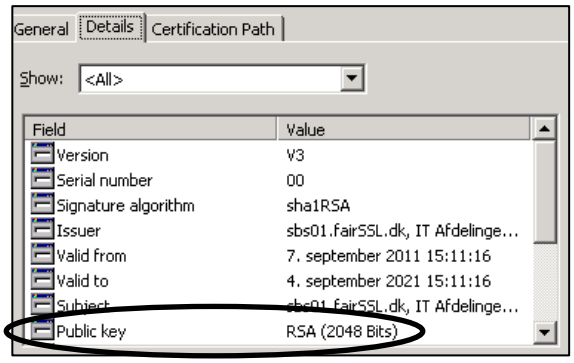
4. Vælg fanebladet ”Directory Security”.

5. Vælg ”View Certificates”.



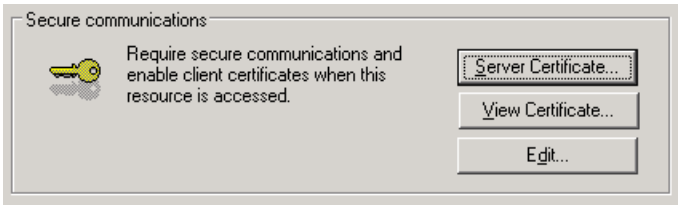
6. Det sikres at certifikatet er udstedt med en ”Public key” på RSA (2048 Bits).

   Er certifikatet udstedt med 1024 Bits eller mindre, stat guiden ”Nyt certifikat på fiktivt website”.

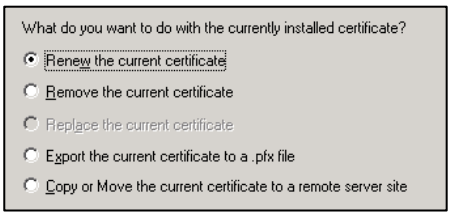


FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

7. Vælg ”Server Certificate”.



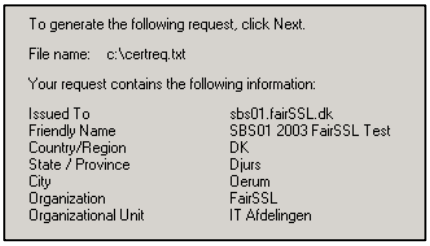
8. Vælg ”Renew the current certificate”.



9. Vælg ”Prepare the request now, but send it later”.

10. Vælg en placering af din CSR fil.

11. Overblik over indtastningerne.



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

13. Når certifikatet er modtaget, start guiden ”**Afslutning af afventende certifikat request**”.

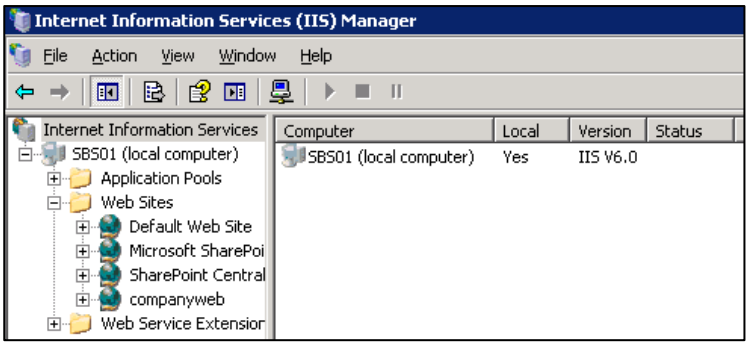
FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Nyt certifikat på fiktivt website

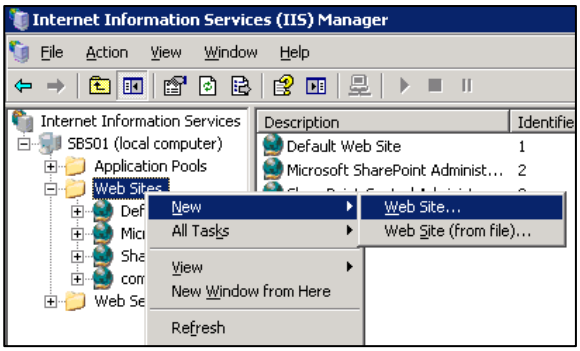
Følgende beskriver hvordan man genbestiller et certifikat der er udstedt med en "Public key" på RSA (1024 Bits) eller mindre.
Denne løsning sørger for at der ikke er nedetid på et produktivt website.

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

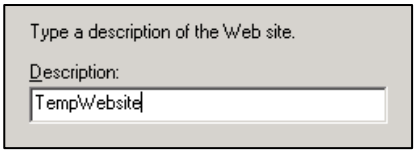
2. Under "Administrative Tools" startes "Internet Information Services (IIS) Manager"



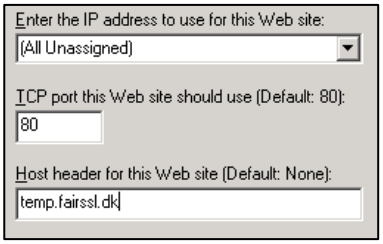
3. Højre klik på "Web Sites" og vælg "New -> Web Site".



4. Vælg et navn til det nye midlertidige website.



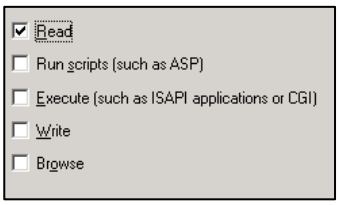
5. Vælg IP, Port og Host header.



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

6. Vælg placering af filer.

7. Tildel rettigheder på websitet.



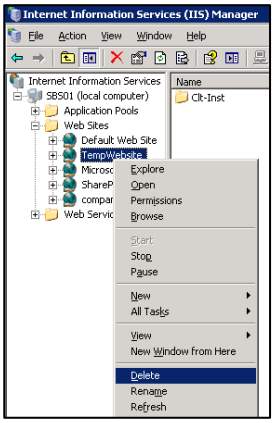
8. Gennemfør afsnittet "**Generering af CSR til certifikat bestilling**" på det nye website.

9. Gennemfør afsnittet " **Import af mellemudsteder certifikat ("Intermediate Certificate Authority")**"

10. Gennemfør afsnittet "**Afslutning af afventende certifikat request**" på det nye website.

11. Gennemfør afsnittet "**Opsætning af installeret certifikat på website**", og sæt certifikatet op til det rigtige website.

12. Slet det midlertidige website.



13. Certifikatet er nu opsat og i drift.

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