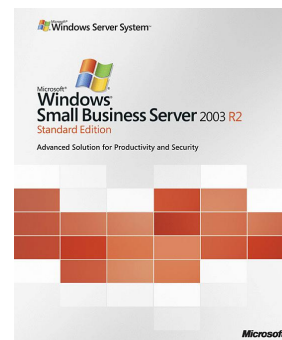


## Small Business Server 2003 Certifikat administration

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](mailto:support@fairssl.dk) eller telefon +45 77 345 678. For certifikat bestilling, certifikat sammenligninger og flere vejledninger se websitet på [www.fairssl.dk](http://www.fairssl.dk).

Husk at teste din installation når du er færdig gratis på [www.fairssl.dk/ssltest/](http://www.fairssl.dk/ssltest/)

## Indholdsfortegnelse

Small Business Server 2003 Certifikat administration.....	1
Valg af certifikat.....	1
Generering af CSR til certifikat bestilling.....	3
Import af mellemsteder certifikat ("Intermediate Certificate Authority").....	6
Afslutning af afventende certifikat request .....	8
Import af certifikat udstedt med AutoCSR (.PFX).....	10
Opsætning af installeret certifikat på website .....	12
Fornyelse af certifikat med CSR.....	14
Nyt certifikat på fiktivt website .....	16

### VIGTIG INFORMATION – LÆS MIG!

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

## 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

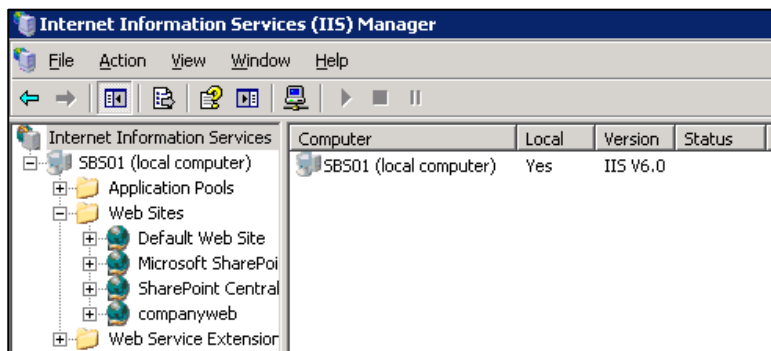
- Companyweb (Anvendes af sharepoint)
- Servernavn
- Servernavn.Domænenavn



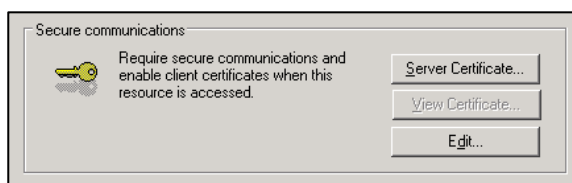
## Generering af CSR til certifikat bestilling

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

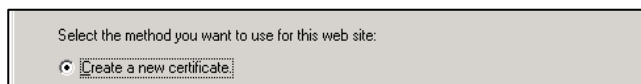
1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.
2. Under "Administrative Tools" startes "Internet Information Services (IIS) Manager"



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! Henvissningskilde 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".



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

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length:

Select cryptographic service provider (CSP) for this certificate

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.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:

Organizational unit:

11. Navnet på det domæne certifikatet skal anvendes på.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:

12. Navnet på land, region og by indtastes

Country/Region:

State/province:

City/locality:

State/province and City/locality must be complete, official names and may not contain abbreviations.

13. Vælg en placering af din CSR fil.

Enter a file name for the certificate request.

File name:

## 14. Overblik over indtastningerne.

To generate the following request, click Next.

File name: c:\certreq.txt

Your request contains the following information:

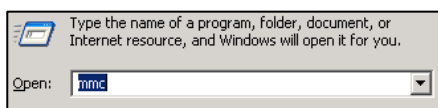
Issued To	sbs01.FairSSL.dk
Friendly Name	SBS01 2003 FairSSL Test
Country/Region	DK
State / Province	Djurs
City	Oerum
Organization	FairSSL
Organizational Unit	IT Afdelingen

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

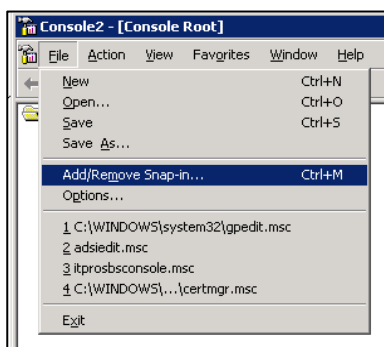
## Import af mellemsteder certifikat ("Intermediate Certificate Authority")

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

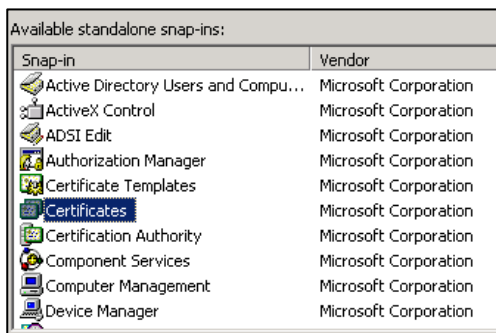
1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.
2. Kopier teksten med mellemsteder certifikatet ("Intermediate certificate"), fra e-mailen med dit nye certifikat, til en simpel tekst editor (som Notepad). Gem filen på skrivebordet, med filnavnet "mellemsteder.cer".
3. Vælg Start – Kør og skriv følgende kommando "mmc.exe".



4. Vælg "Add/Remove Snap In".



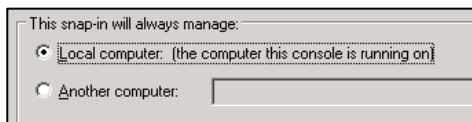
5. Vælg "Add".
6. Tilføj "Certificates".



7. Vælg "Computer Account".

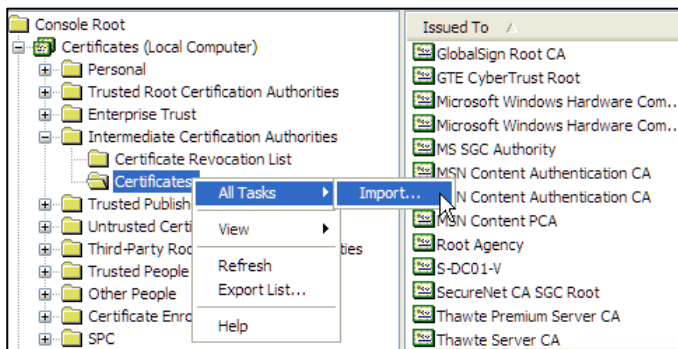


8. Vælg "Local Computer".

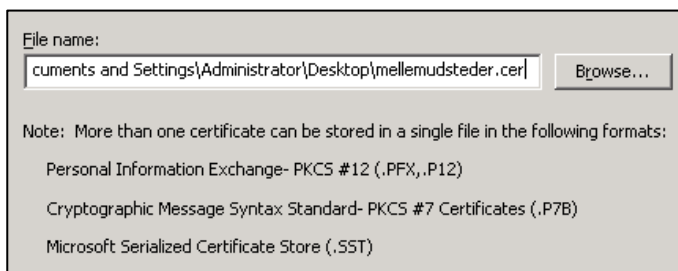


9. Under "Certificates (Local Computer)" udvid "Intermediate Certification Authorities" og "Certificates".

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"

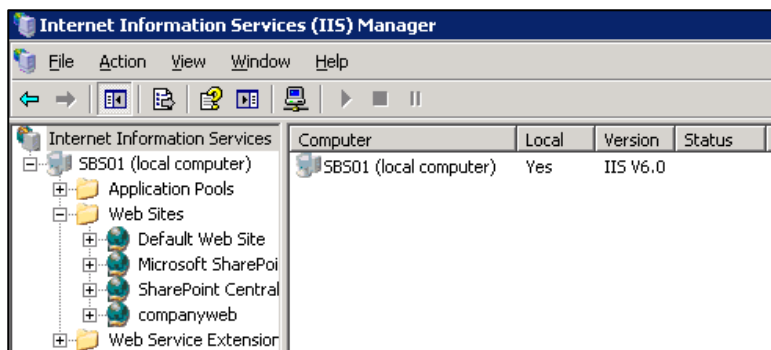


13. Mellemsteder certifikatet er nu importeret.

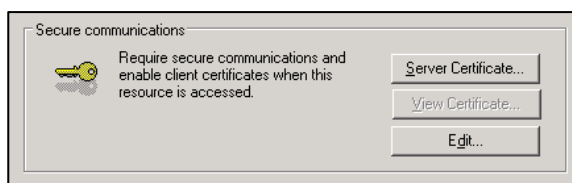
## Afslutning af afventende certifikat request

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

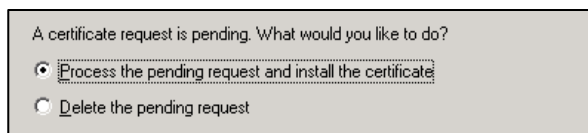
1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.
2. Kopier teksten med certifikatet, fra e-mailen med dit nye certifikat, til en simpel tekst editor (som Notepad). Gem filen på skrivebordet med et passende filnavn, og en endelse på ".cer" eller ".pem". 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".



8. Vælg filen som tidligere blev gemt på skrivebordet.

Enter the path and file name of the file containing the certification authority's response.

Path and file name:

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

SSL port this web site should use:

10. Overblik over det valgte certifikat.

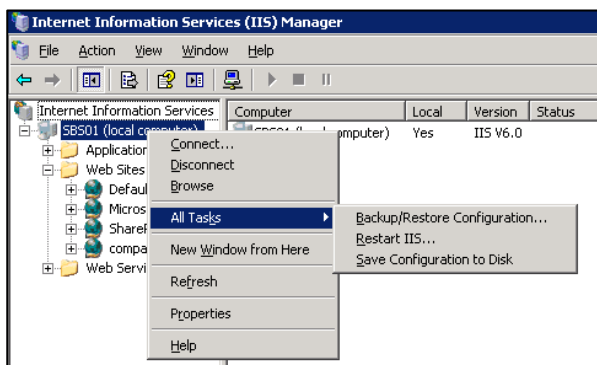
To install the following certificate, click Next.

File name: C:\Documents and Settings\Administr...\SBS01-FairSSL.dk.cer

Certificate details:

Issued To	sbs01.fairSSL.dk
Issued By	www.FairSSL.dk
Expiration Date	02-09-2012
Friendly Name	SBS01 2003 FairSSL Test
Country/Region	DK
State / Province	Djurs
City	Oerum
Organization	FairSSL
Organizational Unit	IT Afdelingen

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



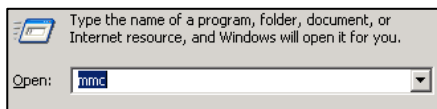
12. Certifikatet er nu aktiveret på websitet.

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

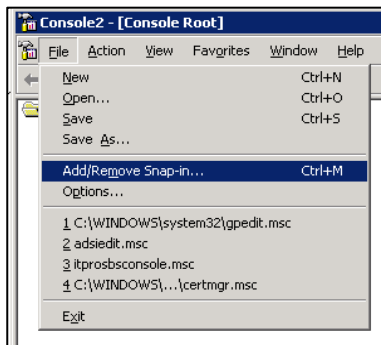
## Import af certifikat udstedt med AutoCSR (.PFX)

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.

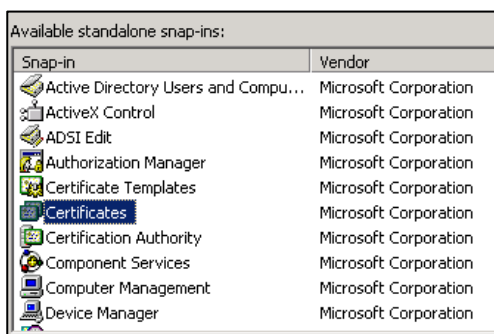
1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.
2. Gem den modtagne fil på skrivebordet.
3. Vælg Start – Kør og skriv følgende kommando "mmc.exe".



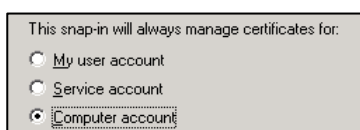
4. Vælg "Add/Remove Snap In".



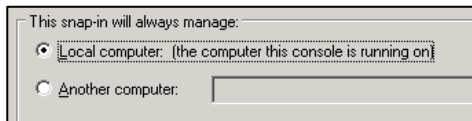
5. Vælg "Add".
6. Tilføj "Certificates".



7. Vælg "Computer Account".

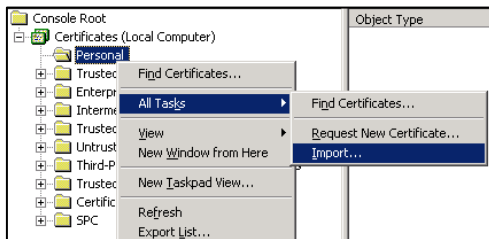


8. Vælg "Local Computer".

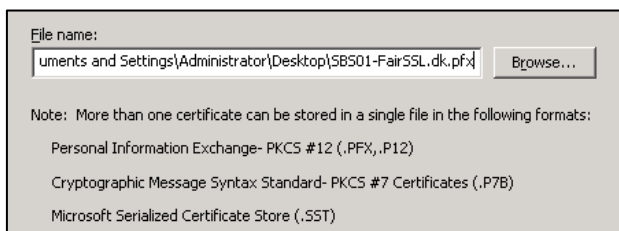


9. Under "Certificates (Local Computer)" udvid "Personal".

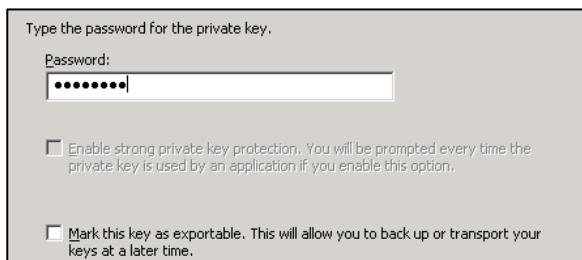
10. Højre klik på "Personal" og vælg "All-Tasks" og "Import".



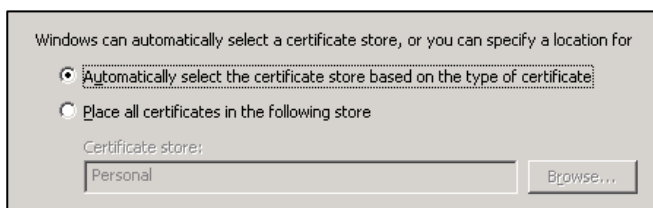
11. Vælg filen som tidligere blev gemt på skrivebordet.



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".

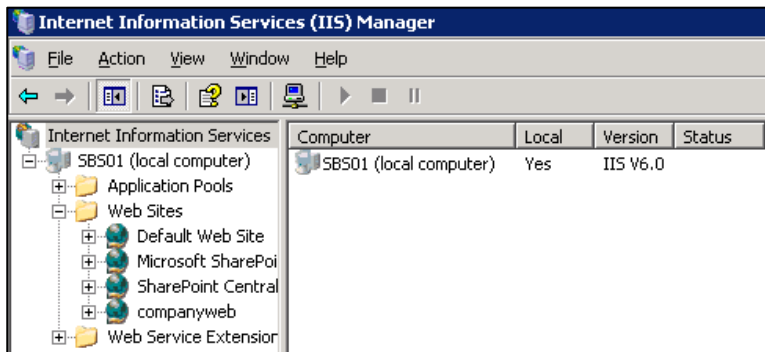


14. Certifikatet er nu importeret.

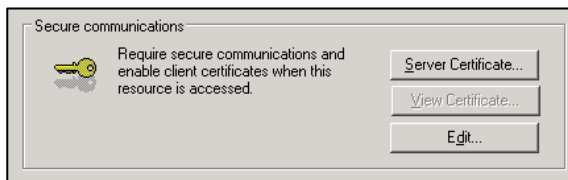
## Opsætning af installeret certifikat på website

Følgende beskriver hvordan et allerede installeret certifikat tilknyttes et website.

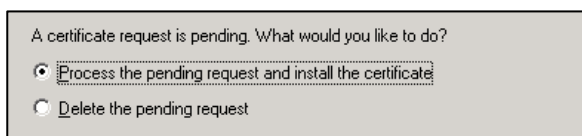
1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.
2. Under "Administrative Tools" startes "Internet Information Services (IIS) Manager"



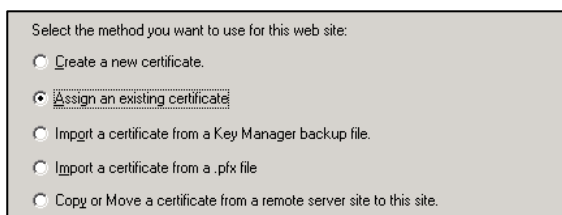
3. Højre klik på det ønskede website ("Default Web Site"), og vælg egenskaber ("Properties").
4. Vælg fanebladet "Directory Security".
5. Vælg "Server Certificate".



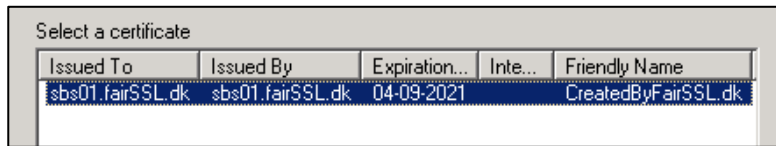
6. Herefter starter en certifikatguide. Vælg "Process the pending request and install the certificate".



7. Vælg "Assign an existing certificate"



8. Vælg det certifikat der skal bruges på websitet.



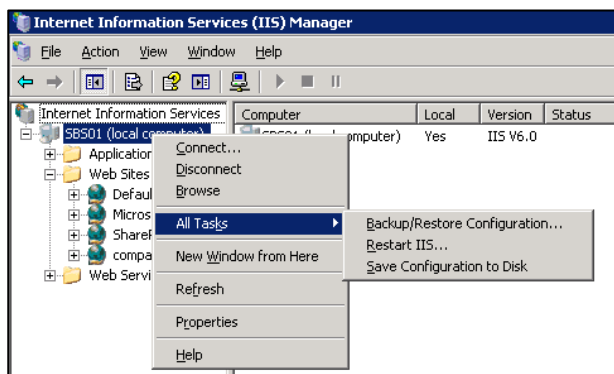
9. Vælg den port der skal bruges til HTTPS trafik, som standard benyttes port 443.



10. Overblik over det valgte certifikat.



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



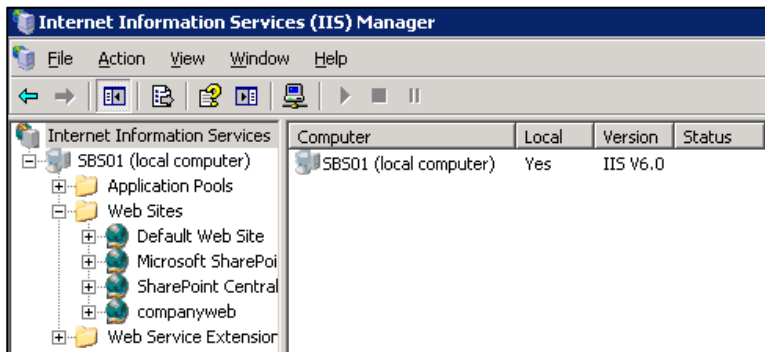
12. Certifikatet er nu aktiveret på websitet.

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

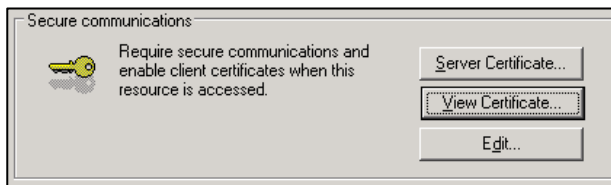
## Fornyelse af certifikat med CSR

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"

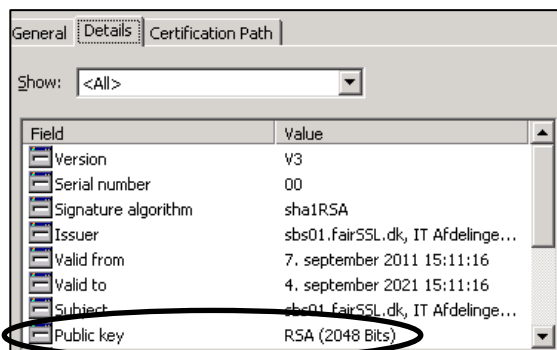


3. Højre klik på det ønskede website ("Default Web Site"), og vælg egenskaber ("Properties").
4. Vælg fanebladet "Directory Security".
5. Vælg "View Certificates".

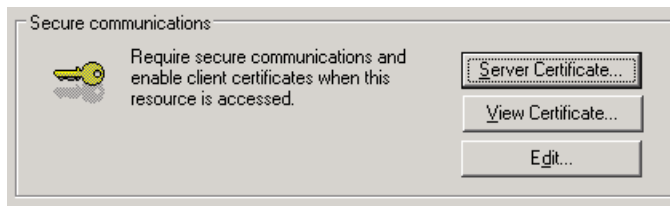


6. Det sikres at certifikatet er udstedt med en "Public key" på RSA (2048 Bits).

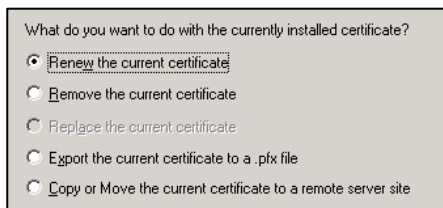
Er certifikatet udstedt med 1024 Bits eller mindre, stat guiden "[Nyt certifikat på fiktivt website](#)".



## 7. Vælg "Server Certificate".



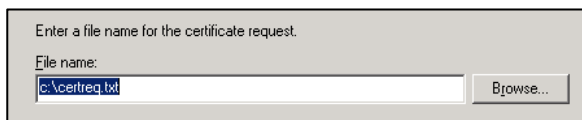
## 8. Vælg "Renew the current certificate".



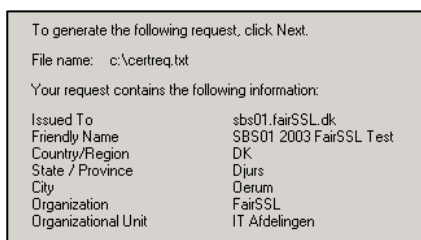
## 9. Vælg "Prepare the request now, but send it later".



## 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.

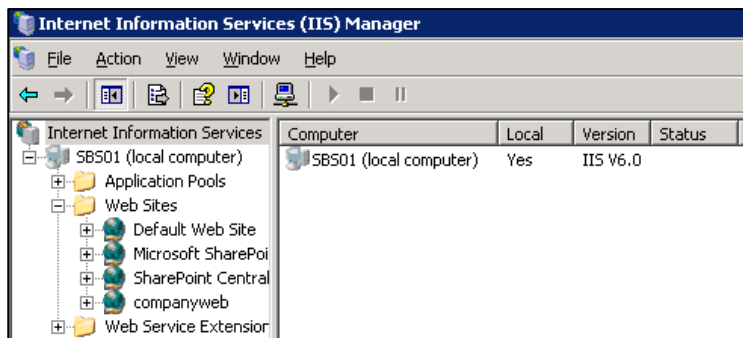
## 13. Når certifikatet er modtaget, start guiden "[Afslutning af afventende certifikat request](#)".

## Nyt certifikat på fiktivt website

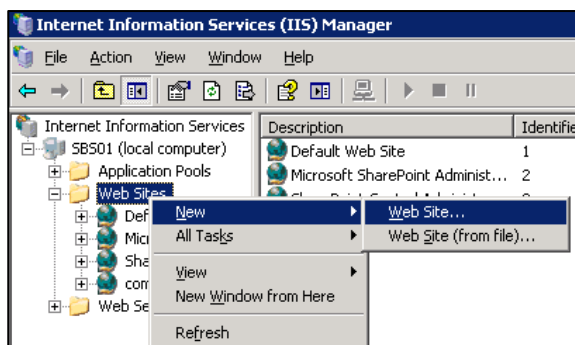
Følgende beskriver hvordan man genbestiller et certifikat der er udstedt med en "Public key" på RSA (1024 Bits) eller mindre.

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.

Type a description of the Web site.

Description:

5. Vælg IP, Port og Host header.

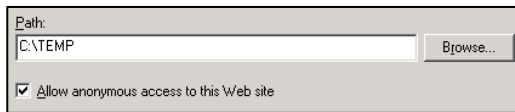
Enter the IP address to use for this Web site:

(All Unassigned)

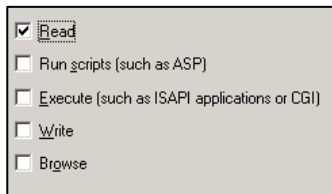
TCP port this Web site should use (Default: 80):

Host header for this Web site (Default: None):

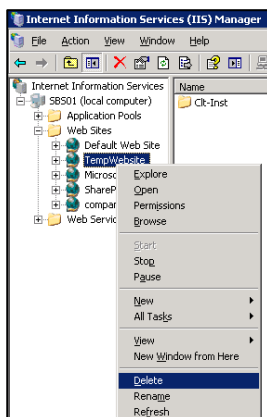
6. Vælg placering af filer.



7. Tildel rettigheder på websitet.



8. Gennemfør afsnittet "[Generering af CSR til certifikat bestilling](#)" på det nye website.
9. Gennemfør afsnittet "[Import af mellemsteder 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/>.