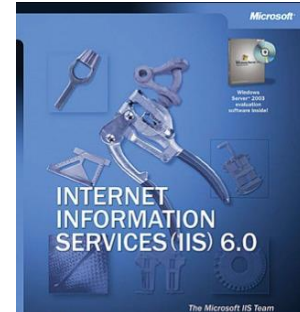


## Microsoft IIS 6 Certifikat administration

Följande guide beskriver hur man installerar ett certifikat på en IIS 6.

För support och hjälp till användandet av denna guide kan du kontakta blueSSL på email [info@bluessl.com](mailto:info@bluessl.com) eller telefon +46 (0)10-10 10 334 eller telefon +45 77 345 678. För beställning av certifikat, jämförelse av certifikat och fler guider titta på vår hemsida [www.bluessl.com](http://www.bluessl.com).



### Inledning

Denna guide beskriver de vanligaste konfigurationerna rörande SSL certifikatshanteringen på en IIS 6. Man kan läsa guiden i sin helhet som en liten guide, eller så kan man ha den som ett sorts uppslagsverk. De första kapitlen täcker den vanligaste hanteringen såsom skapa en CSR, installation av mellanliggande certifikat och slutligen själva installationen av certifikatet.

De andra kapitlen under avancerat är lite mera djuplodande om situationer man kan behöva få en guidning genom. T.ex. om temporära websidor då man skall byta certifikat utan att störa den befintliga produktionsmiljön.

Avslutningsvis bör ni efter all konfiguration testa er certifikatinstallation gratis på [www.bluessl.com/sv/ssltest](http://www.bluessl.com/sv/ssltest).

### Viktig information – LÄS MIG!

Omstart av server eller omstart av tjänster kan vara nödvändig efter installation för att ändringarna från guiden skall synas.

## Innehållsförteckning

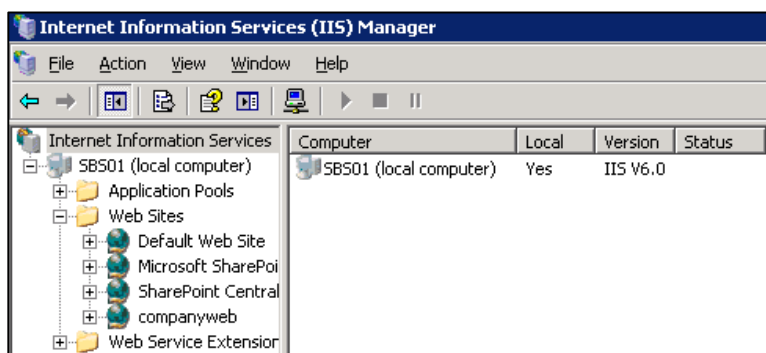
Inledning .....	1
Generering av CSR till ny beställning av certifikat .....	3
Import av mellanliggande certifikat ("Intermediate Certificate Authority") .....	6
Installation av certifikat från en CSR (Certificate Signing Request) .....	8
Avancerat .....	10
Import av PKCS#12 certifikat (AutoCSR, PFX, PKCS#12, Certifikatbackup) .....	10
Skifta mellan installerade SSL certifikat på en websida .....	13
Förnyelse av certifikat med CSR .....	15
Nytt certifikat på en temporär websida .....	17

## Generering av CSR till ny beställning av certifikat

Följande kapitel beskriver hur man gör en Certificate Signing Request (CSR) på en Microsoft Internet Information Server 6.

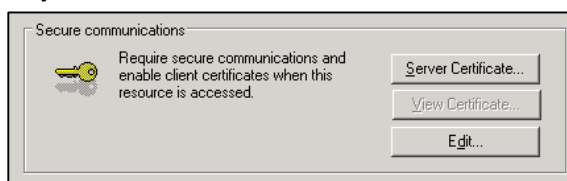
Lägg märke till att certifikat tillverkade utifrån en CSR kan endast installeras på samma maskin, samt att generering av ny CSR på samma maskin gör att föregående CSR blir inaktuell och obrukbar. Avsluta därför alltid en certifikats förfrågan, innan nya CSR tillverkas på samma maskin.

1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Under "Administrative Tools" startas "Internet Information Services (IIS) Manager".

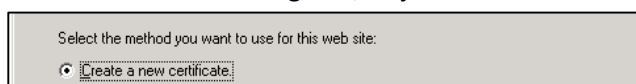


3. Högerklicka på den önskade websidan och välj egenskaper ("Properties").  
**Lägg märke till att om du inte vill påverka denna websidans existerande SSL Certifikat, bör du först utföra "[Nytt certifikat på en temporär websida.](#)" kapitlet av denna vägledning.**

4. Välj fliken "Directory Security".
5. Välj "Server Certificate".



6. Nu startar en certifikatsguide, välj "Create a new Certificate".



7. Välj "Prepare the request now, but send it later".



8. Välj ett passande namn till certifikatet, och "Bit length" ökas till **minst 2048**.

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

Name:  
SBS01 2003 FairSSL Test

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: 2048

Select cryptographic service provider (CSP) for this certificate

9. Fyll i upplysningar för certifikatet som skickas till utfärdaren. Alla exempel nedan är med FairSSL som exempel och bör givetvis rättas till så det passar Ert företag. För att vara säkert på att certifikatet utfärdas utan problem bör man undvika "ÅÄÖ" och andra specialtecken.

10. Fyll i firmanamn och eventuell avdelning.

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:  
FairSSL

Organizational unit:  
IT Avdelningen

11. Namnet på den domän som certifikatet skall användas 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:  
sbs01.fairssl.dk

12. Namnet på land, region och stad ifylles.

Sverige använder Ni länet som region, glöm ej att undvika "ÅÄÖ".

Country/Region:  
DK (Denmark)

State/province:  
Djurs

City/locality:  
Oerum

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

13. Välj en placering av din CSR fil.

Enter a file name for the certificate request.

File name:  
c:\certreq.txt

Browse...

## 14. Nu får Ni en överblicka av Er inmatning.

```
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               Derum  
Organization       FairSSL  
Organizational Unit IT Afdelingen
```

## 15. Ni har nu upprättat en CSR som kan användas till Er certifikats beställning.

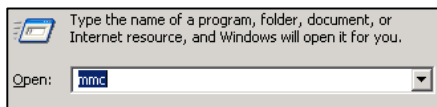
När ni mottagit Ert certifikat skall följande kapitel följas:

- [Import av mellanliggande certifikat \("Intermediate Certificate Authority"\)](#).
- [Installation av certifikat från en CSR \(Certificate Signing Request\)](#).

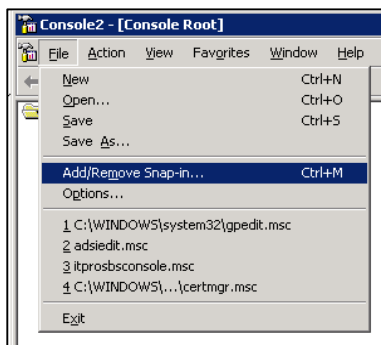
## Import av mellanliggande certifikat ("Intermediate Certificate Authority").

Följande kapitel beskriver hur Ni installerar det mellanliggande certifikatet på Microsoft Windows baserad server och därmed också på en IIS 6. För att vara säker på att klienterna kan godkänna mellanliggande certifikat, skall certifikatets mellanliggande offentliga certifikat installeras på servern. Vid leverans av ett GlobalSign certifikat, får Ni också med det offentliga mellanliggande certifikatet.

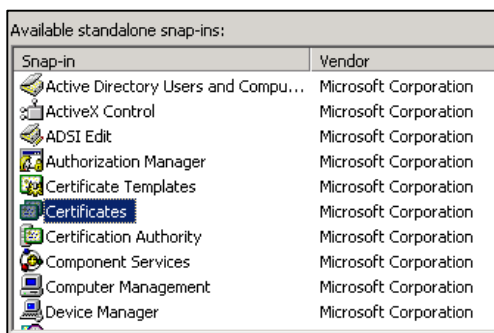
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Kopiera texten med det mellanliggande certifikatet ("Intermediate certificate"), från mailen med Ert nya certifikat, till en simpel texteditor (Notepad). Spara filen på skrivbordet, med filnamnet "mellanliggande.cer".
3. Välj "Start" – "Kör" och skriv följande kommando "mmc.exe".



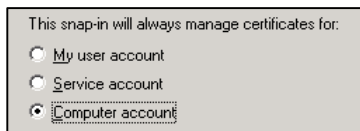
4. Välj "Add/Remove Snap In".



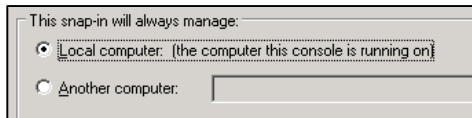
5. Välj "Add"
6. Lägg till "Certificates"



7. Välj "Computer Account"

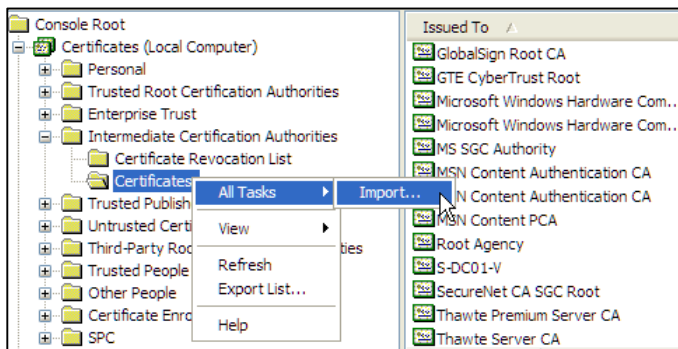


8. Välj "Local Computer"

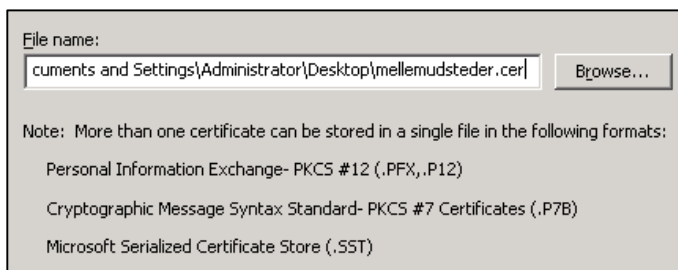


9. Under "Certificates (Local Computer)", expandera "Intermediate Certification Authorities" och "Certificates"

10. Högerklicka på "Certificates" och välj "All-Tasks" och "Import".



11. Välj filen som Ni tidigare sparade på skrivbordet



12. Kontrollera att certifikatet blir sparad i "Intermediate Certification authorities".

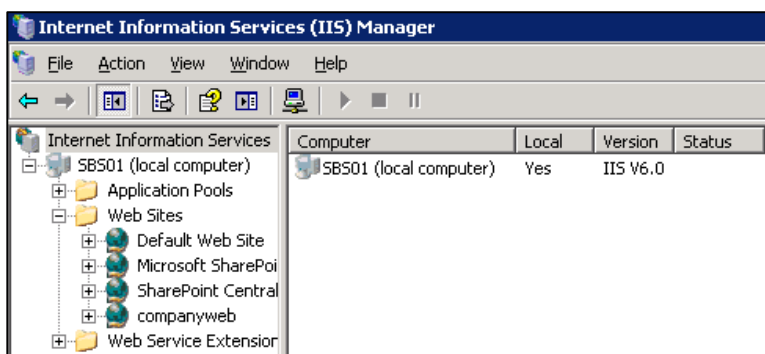


13. Det mellanliggande certifikatet är nu importerat!

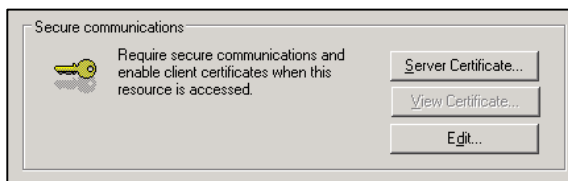
## Installation av certifikat från en CSR (Certificate Signing Request).

Följande kapitel beskriver hur man installerar ett certifikat, efter att det blivit utfärdat från en CSR som Ni genererat på samma server.

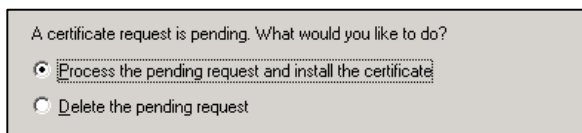
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Kopiera texten med certifikatet, från det e-mail med Ert nya certifikat, till en simpel texteditor (Notepad). Spara filen på Ert skrivbord med ett passande namn, med en ändelse på ".cer" eller ".pem". I exemplet här är filnamnet "SBS01-FairSSL.dk.cer".
3. Under "Administrative Tools" startas "Internet Information Services (IIS) Manager".



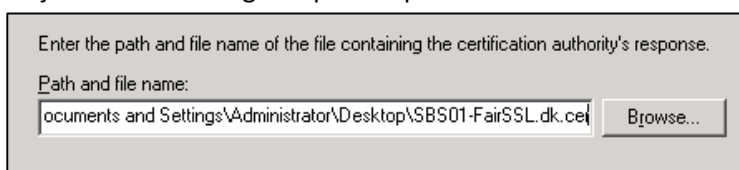
4. Högerklicka på den önskade websidan och välj egenskaper ("Properties").
5. Välj fliken "Directory Security".
6. Välj "Server Certificate".



7. Därmed startas en certifikatguide. Välj "Process the pending request and install the certificate".



8. Välj filen som Ni tidigare sparade på skrivbordet.





9. Välj den port som skall användas till HTTPS trafik, som standard brukar man använda port 443.

SSL port this web site should use:

10. Överblicka det valda certifikatet.

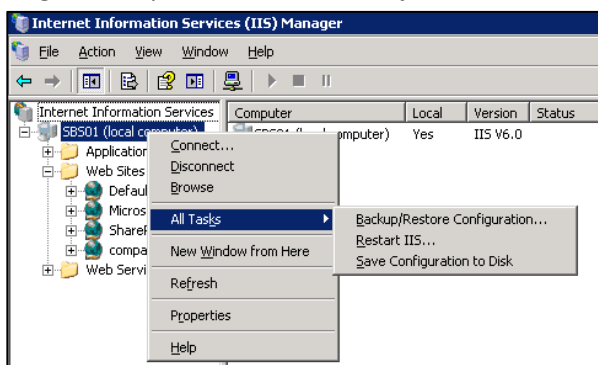
To install the following certificate, click Next.

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	Ørum
Organization	FairSSL
Organizational Unit	IT Afdelingen

11. Högerklicka på IIS servern och välj "All Tasks" och efter detta "Restart IIS..."



12. Certifikatet är nu aktiverat på websidan.

13. Testa så att certifikatet fungerar som det skall på:  
<https://www.fairssl.dk/ssltest/>.

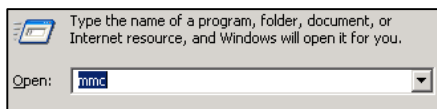
## Avancerat

Följande kapitel som följer är lite mer avancerade uppgifter men som likväl kommer till användning.

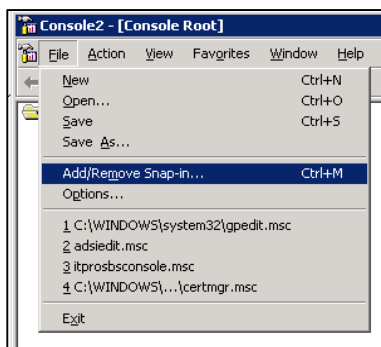
### Import av PKCS#12 certifikat (AutoCSR, PFX, PKCS#12, Certifikatbackup).

Följande beskriver hur Ni installerar ett PKCS#12 SSL certifikat. Vid beställning av certifikat med AutoCSR levereras certifikatet som en backupfil, skyddat med en unik kod.

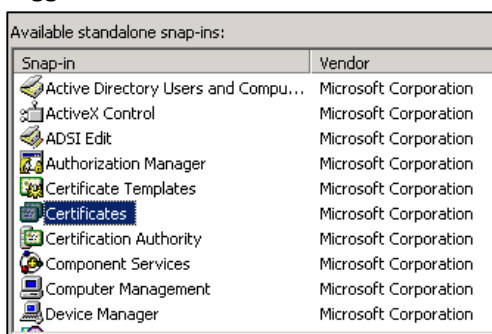
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Spara den mottagna filen på Ert skrivbord.
3. Välj "Start" – "Kör" och skriv följande kommando "mmc.exe"



4. Välj "Add/Remove Snap In".



5. Välj "Add"
6. Lägg till "Certificates"



7. Välj "Computer Account"

This snap-in will always manage certificates for:

My user account

Service account

Computer account

8. Välj "Local Computer"

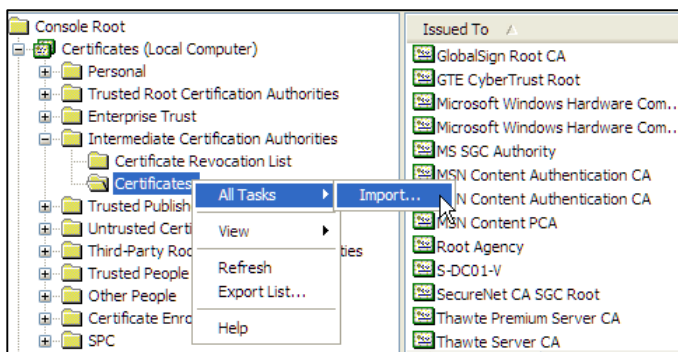
This snap-in will always manage:

Local computer: (the computer this console is running on)

Another computer: \_\_\_\_\_

9. Under "Certificates (Local Computer)", expandera "Personal" och "Certificates".

10. Högerklicka på "Certificates" och välj "All-Tasks" och "Import".



11. Välj den fil som Ni tidigare sparade på Ert skrivbord.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

12. Fyll in den kod Ni erhållit via SMS som certifikatet är krypterat med.

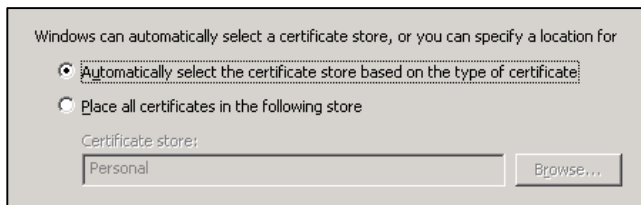
Type the password for the private key.

Password:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

13. Välj "Automatically select the certificate store based on the type of certificate".

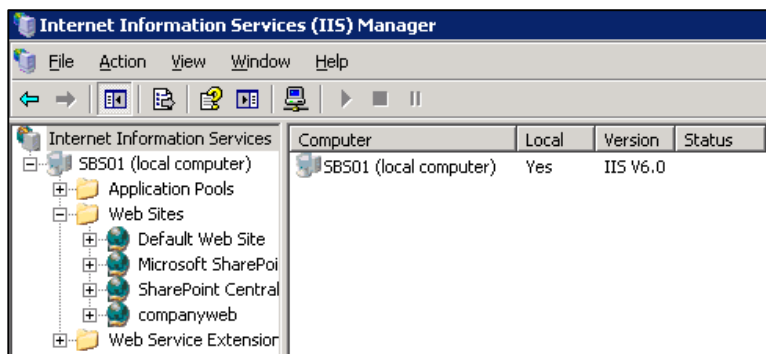


14. Certifikatet är nu importerat.

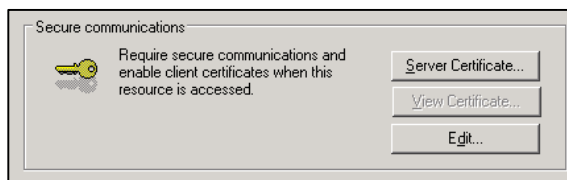
## Skifta mellan installerade SSL certifikat på en websida.

Följande kapitel beskriver hur Ni knyter ett specifikt certifikat till en bestämd websida.

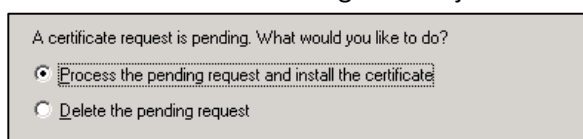
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Under "Administrative Tools" startas "Internet Information Services (IIS) Manager".



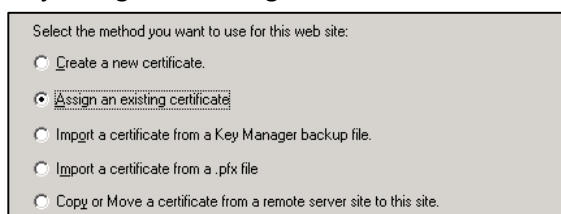
3. Högerklicka på det önskade websidan och välj egenskaper ("Properties").
4. Välj fliken "Directory Security".
5. Välj "Server Certificate".



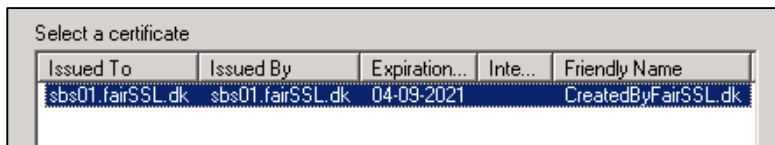
6. Därmed startas en certifikatguide. Välj "Process the pending request and install the certificate".



7. Välj "Assign an existing certificate"



8. Välj det certifikat som skall användas på websidan.



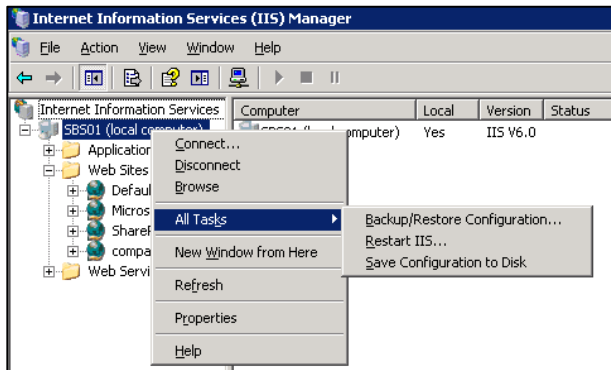
9. Välj den port som skall användas till HTTPS trafiken, vanligtvis används port 443 som standard.



10. Överblicka det valda certifikatet.



11. Högerklicka på IIS servern och välj "All Tasks" och därefter "Restart IIS...".



12. Certifikatet är nu aktiverat på den websidan.

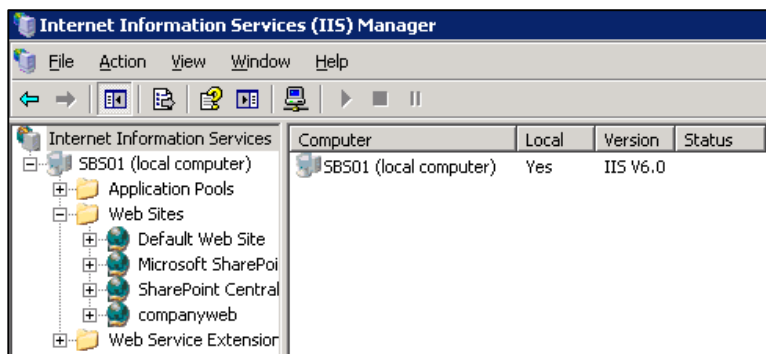
13. Glöm inte att testa certifikatet så det fungerar korrekt på:

<https://www.fairssl.dk/ssltest/>

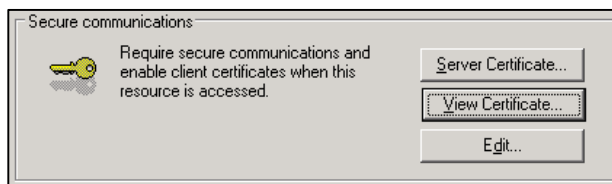
## Förnyelse av certifikat med CSR

Följande kapitel beskriver hur Ni förnyar Ert certifikat på en Websidan

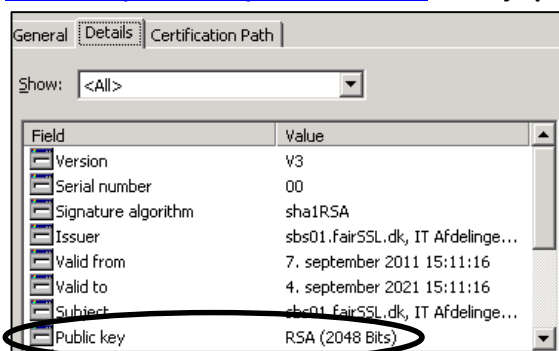
1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Under "Administrative Tools" startas "Internet Information Services (IIS) Manager".



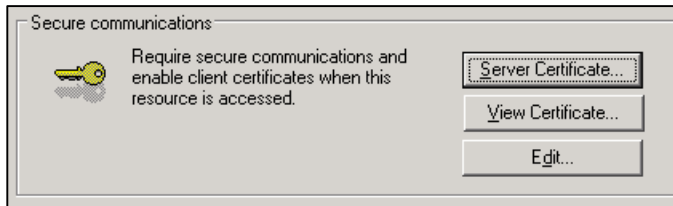
3. Högerklicka på det önskade websidan och välj egenskaper ("Properties").
4. Välj fliken "Directory Security".
5. Välj "View Certificates"



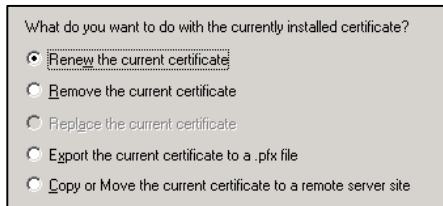
6. Det försäkras att certifikatet är utfärdat med en "Public key" på RSA (2048 Bits).  
**Är certifikatet utfärdat med 1024 bits eller mindre, är förnyelse inte möjligt, se guiden "[Nytt certifikat på en temporär websida.](#)" för hjälp.**



7. Välj "Server Certificate".



8. Välj "Renew the current certificate".



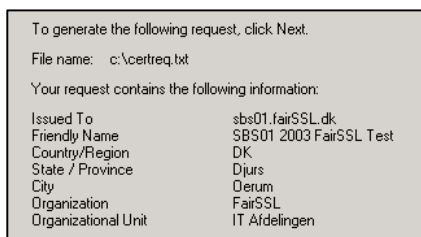
9. Välj "Prepare the request now, but send it later".



10. Välj en placering av din CSR fil.



11. Överblick av ifyllningarna.



12. Ni har nu upprättat en CSR som kan användas till certifikat beställningen.

Efter leverans av certifikatet skall följande kapitel följas:

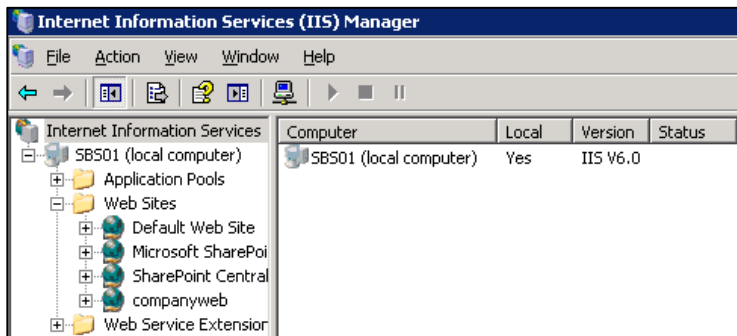
- [Import av mellanliggande certifikat \("Intermediate Certificate Authority"\).](#)
- [Installation av certifikat från en CSR \(Certificate Signing Request\).](#)



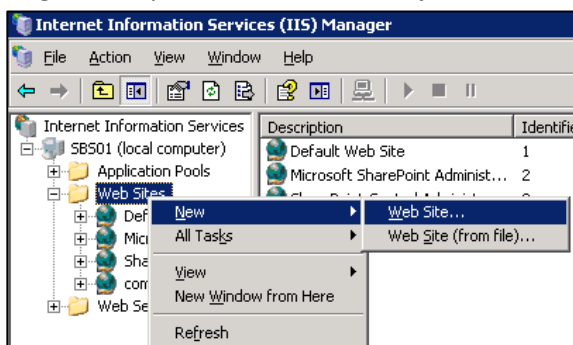
## Nytt certifikat på en temporär websida.

Följande guide beskriver hur man beställer ett SSL certifikat utan att störa det existerande SSL certifikatet som är i produktion på en websida. Lösningen är att man använder en temporär websida som bara används till att beställa och installera certifikatet. Därefter kan man skifta certifikat utan att få någon nedtid.

1. Logga in på servern med ett konto som är medlem av gruppen "Administrators" på den lokala servern.
2. Under "Administrative Tools" startas "Internet Information Services (IIS) Manager".



3. Högerklicka på "Web Sites" och välj "New -> Web Site".



4. Välj ett namn till den temporära sidan.

Type a description of the Web site.

Description:

5. Välj IP, Port och Header.

Enter the IP address to use for this Web site:

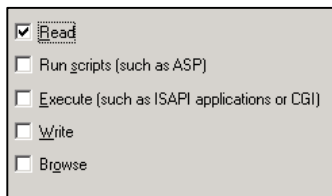
TCP port this Web site should use (Default: 80):

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

6. Välj placering av filer



7. Tilldela rättigheter på websidan.



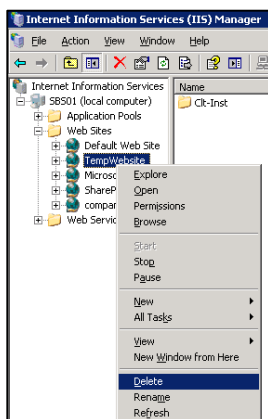
8. Genomför kapitlet "[Generering av CSR till ny beställning av certifikat](#)", på den nya websidan.

9. Genomför kapitlet "[Import av mellanliggande certifikat \('Intermediate Certificate Authority'\)](#)".

10. Genomför kapitlet "[Installation av certifikat från en CSR \(Certificate Signing Request\)](#)".

11. Genomför kapitlet "[Skifta mellan installerade SSL certifikat på en website](#)", där det nya certifikatet väljs för produktionswebsidan.

12. Ta bort den temporära websidan.



13. Testa så att en websidan fungerar som den skall på:

<https://www.fairssl.dk/ssltest/>.