

CÀI ĐẶT – CẤU HÌNH WEBSITE SỬ DỤNG CA

1. Giới thiệu dịch vụ Certificate Services:

Certificate Authority (CA) : là tổ chức phát hành các loại chứng thư số cho người dùng, doanh nghiệp, máy chủ (server), mã code, phần mềm. Nhà cung cấp chứng thư số đóng vai trò là bên thứ ba (được cả hai bên tin tưởng) để hỗ trợ cho quá trình trao đổi thông tin an toàn.

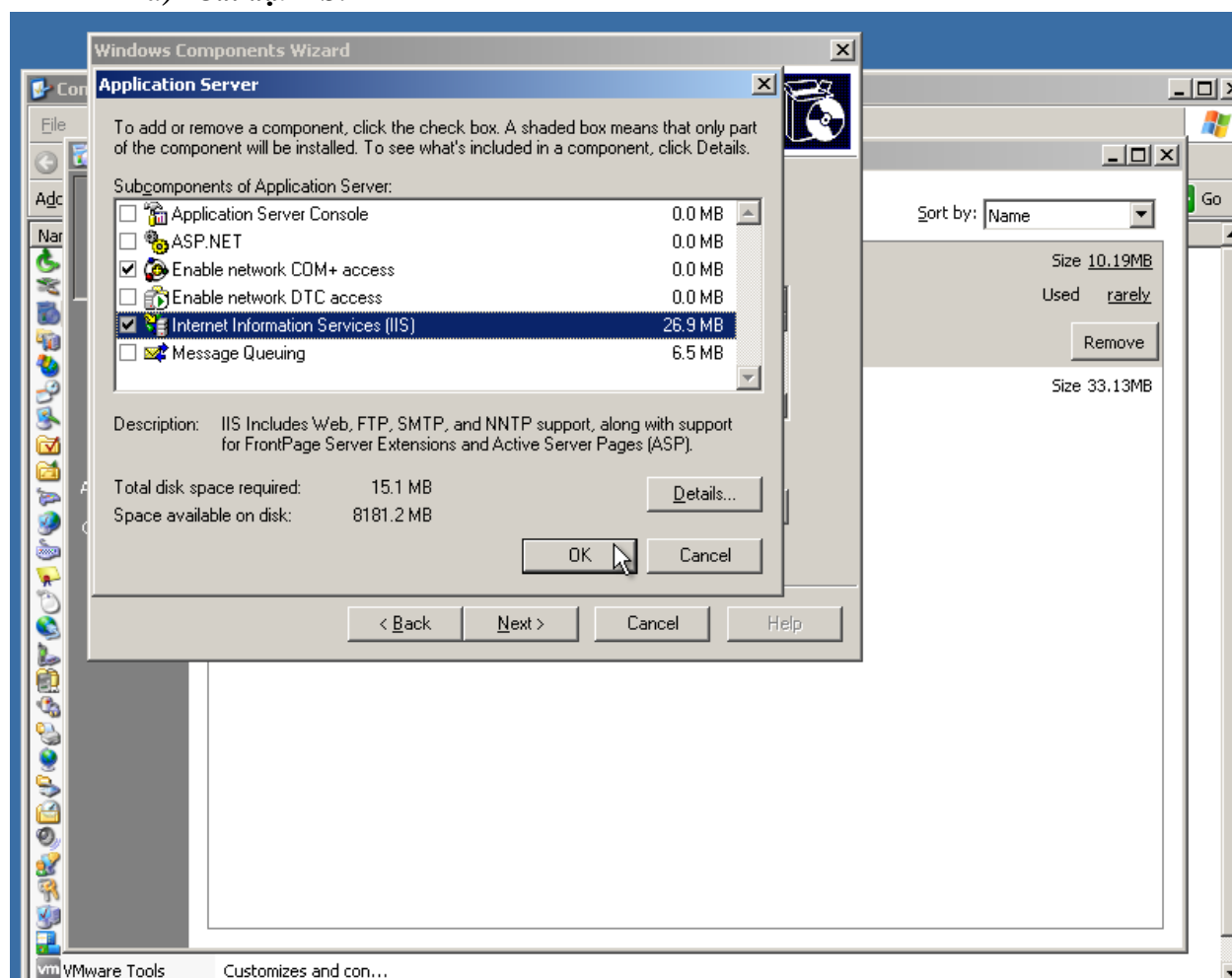
2. Mục tiêu:

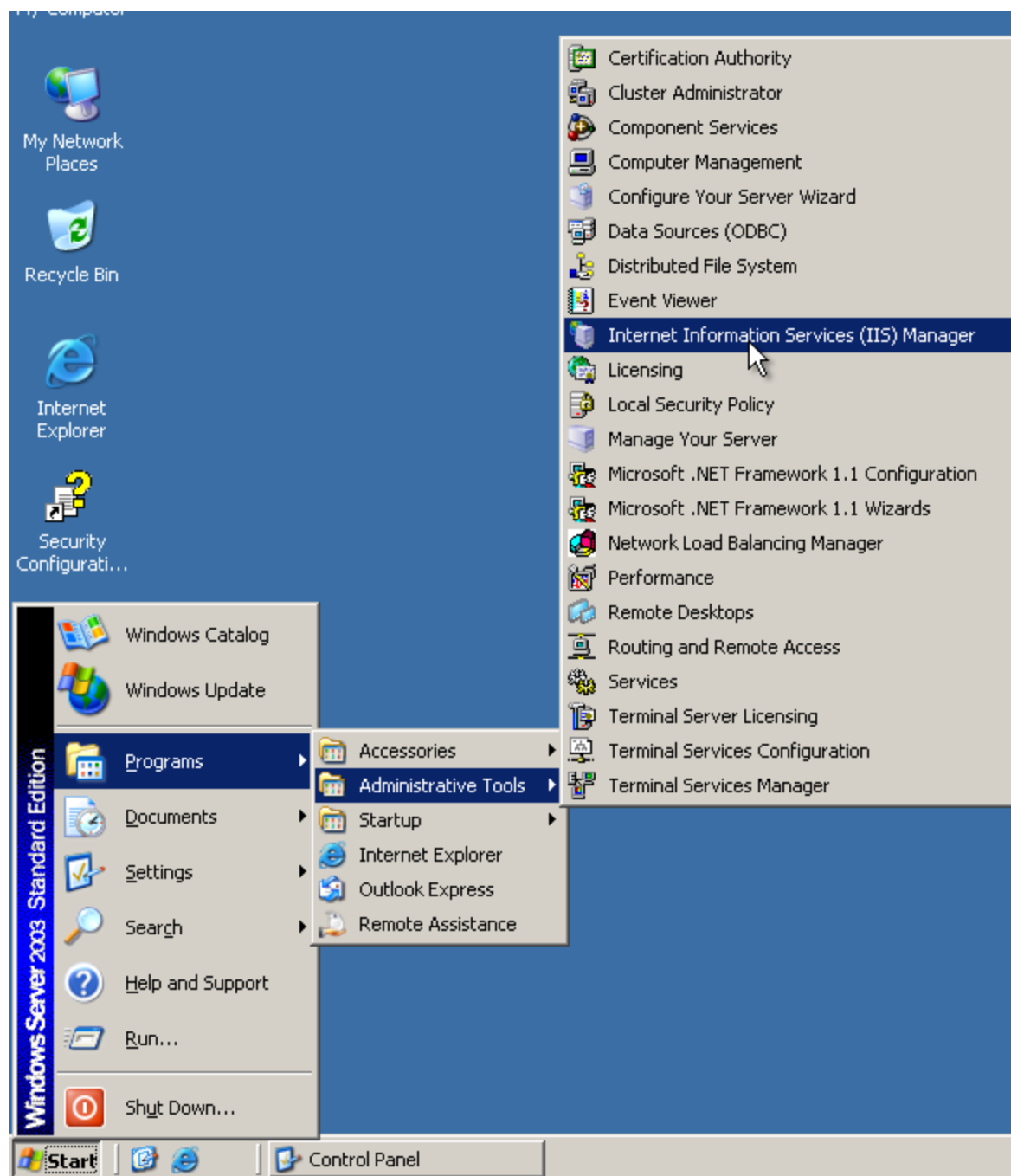
- Tìm hiểu cách cài đặt dịch vụ CA trên window server 2003.
- Cấu hình để 1 website có thể sử dụng chứng chỉ số (certificate) do CA cấp dùng chứng thực với người dùng.

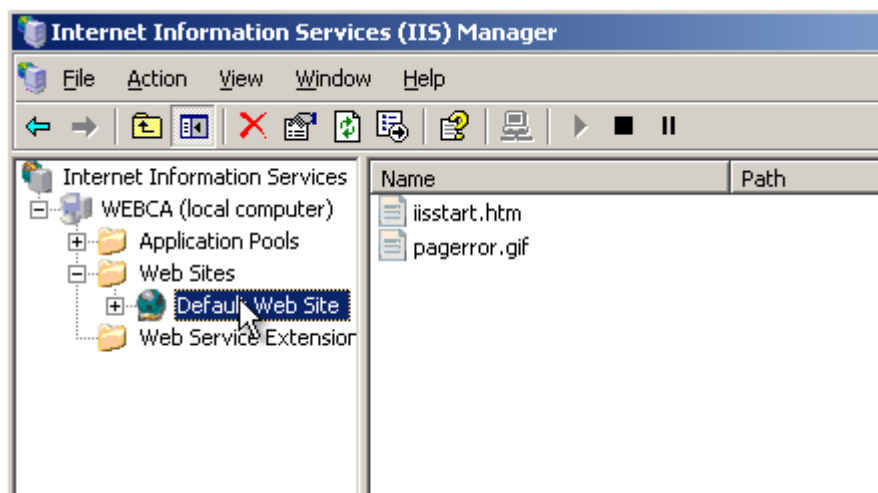
3. Nội dung:

A. Cài đặt:

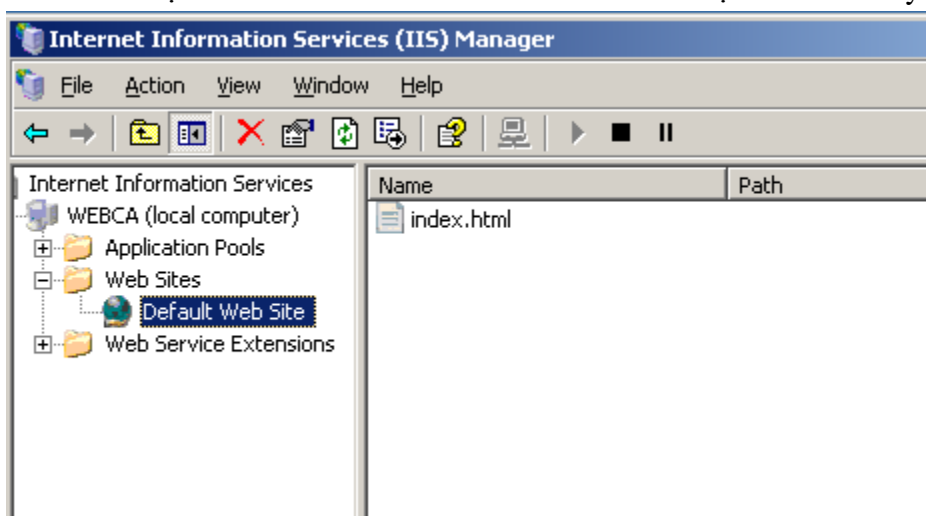
a) Cài đặt IIS:



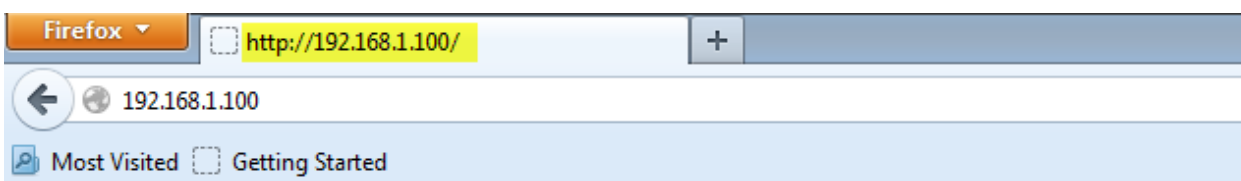




- Tạo file index.html và trở webroot về thư mục chứa file này

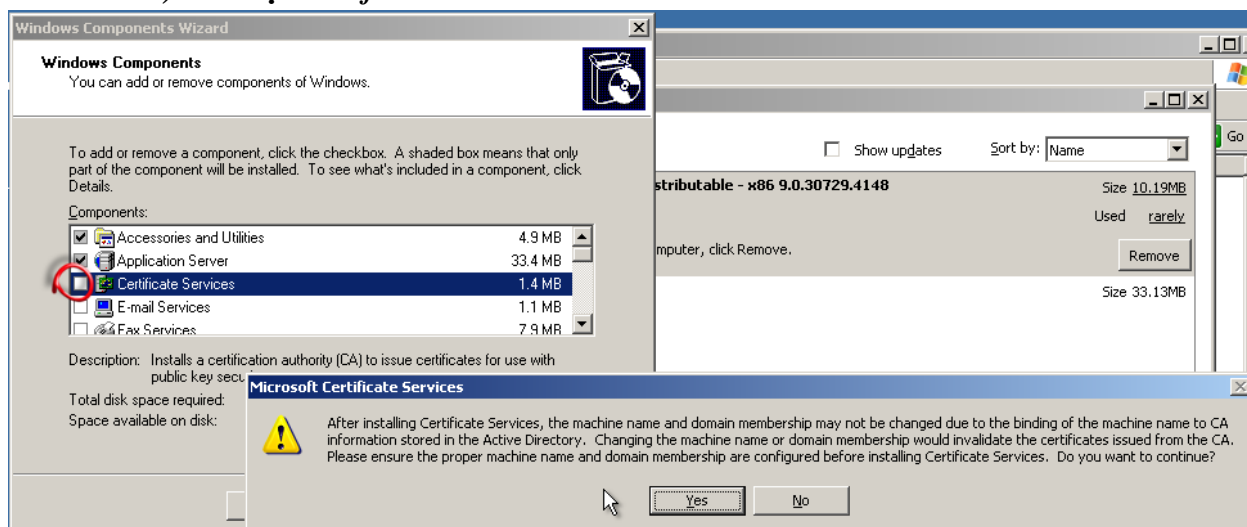


- Kiểm tra: từ máy tính khác vào trình duyệt xem trang web:

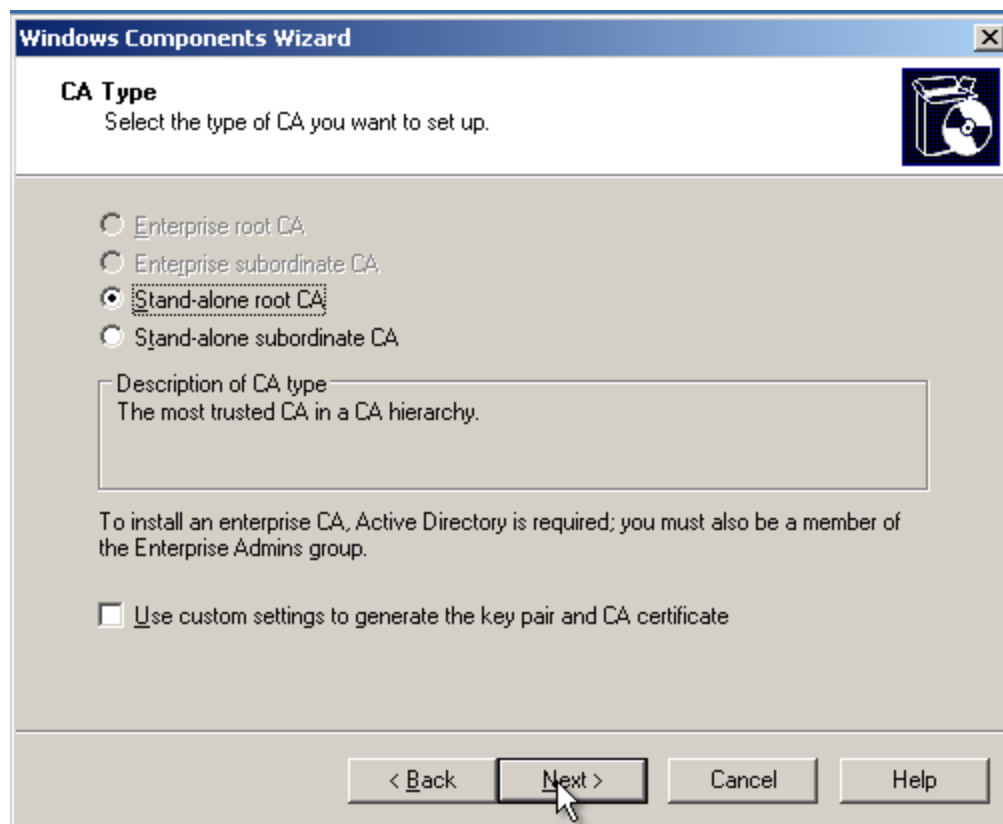


Website TKUDM

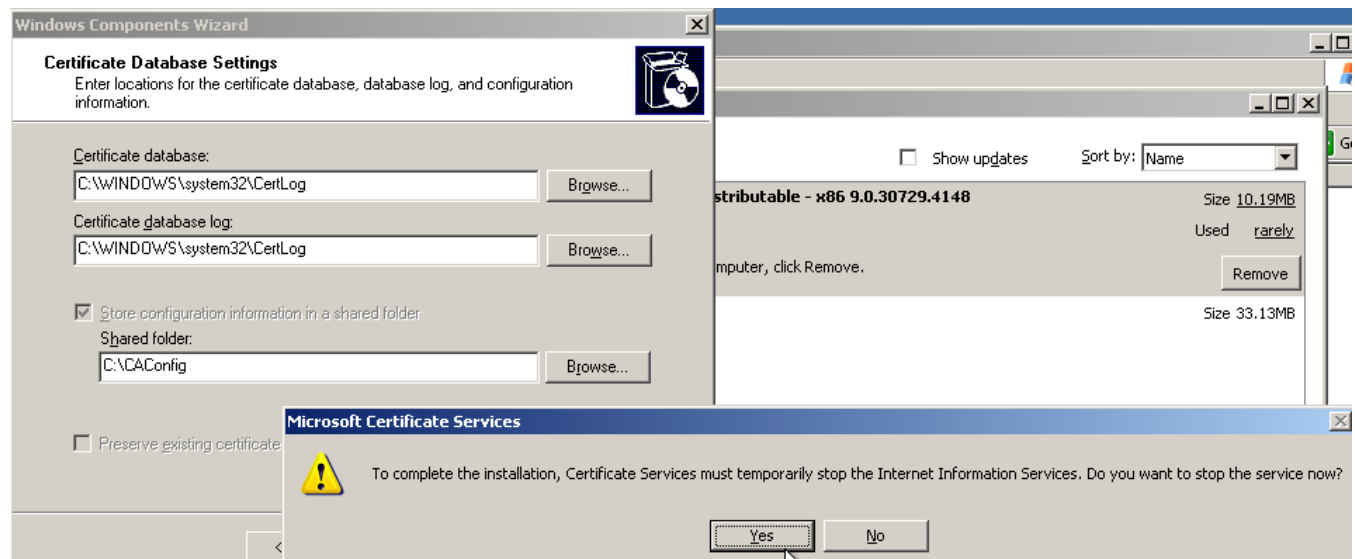
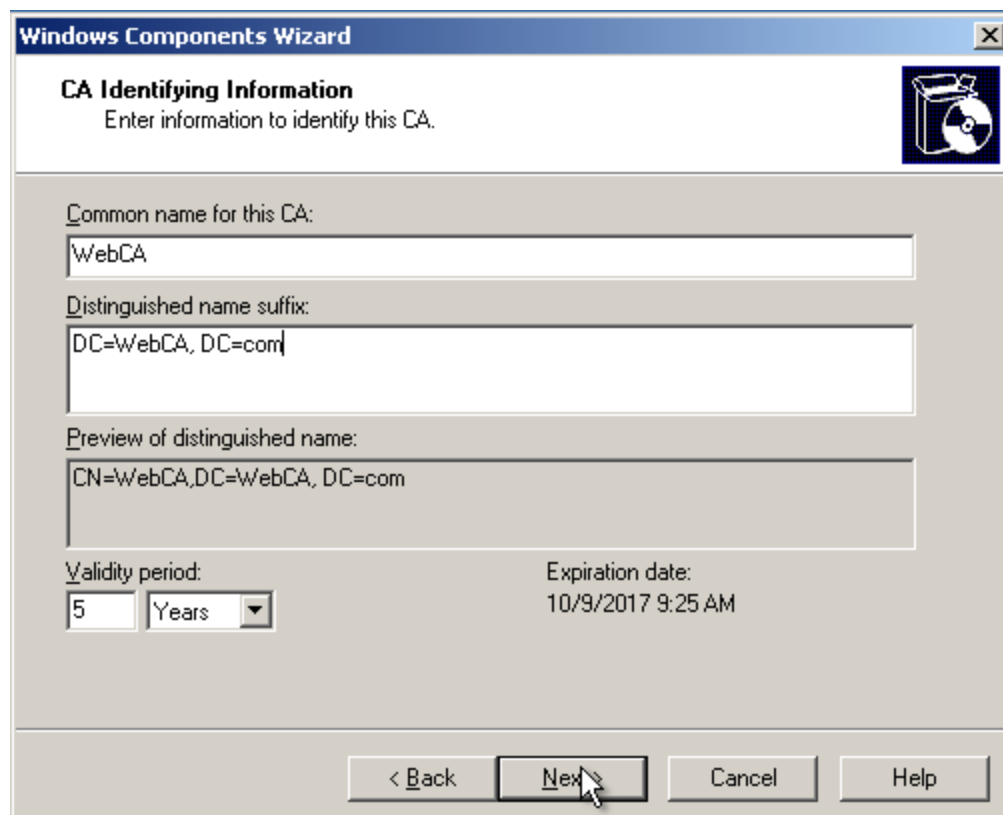
b) Cài đặt Certificate Services:



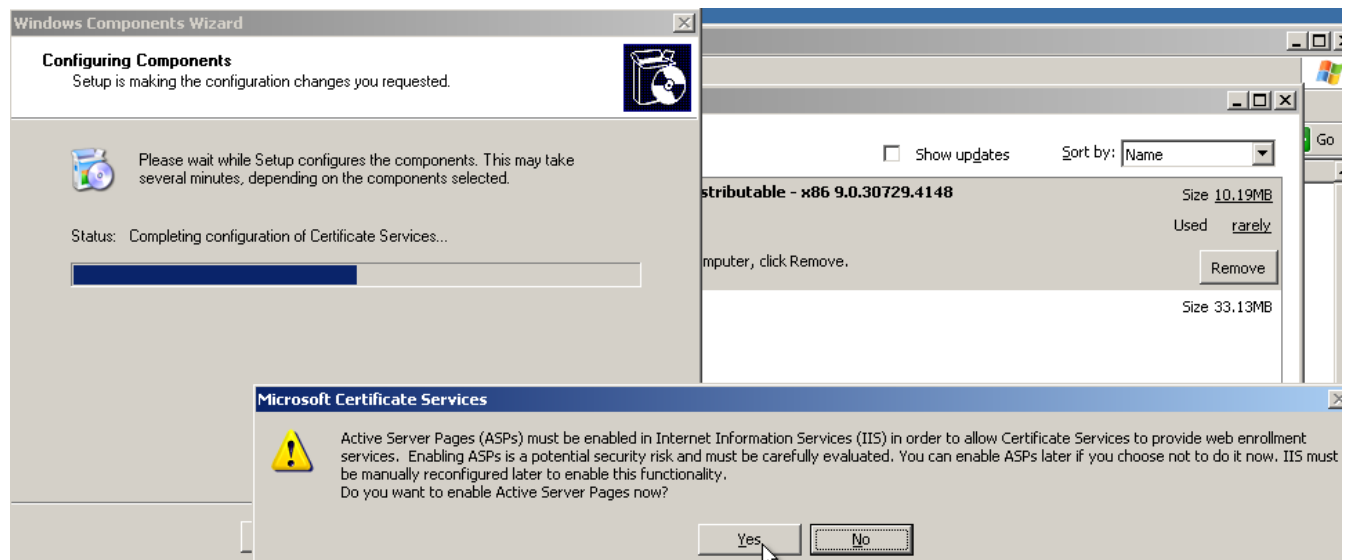
- Do đây là CA server đầu tiên nên ta chọn Stand-alone root CA:

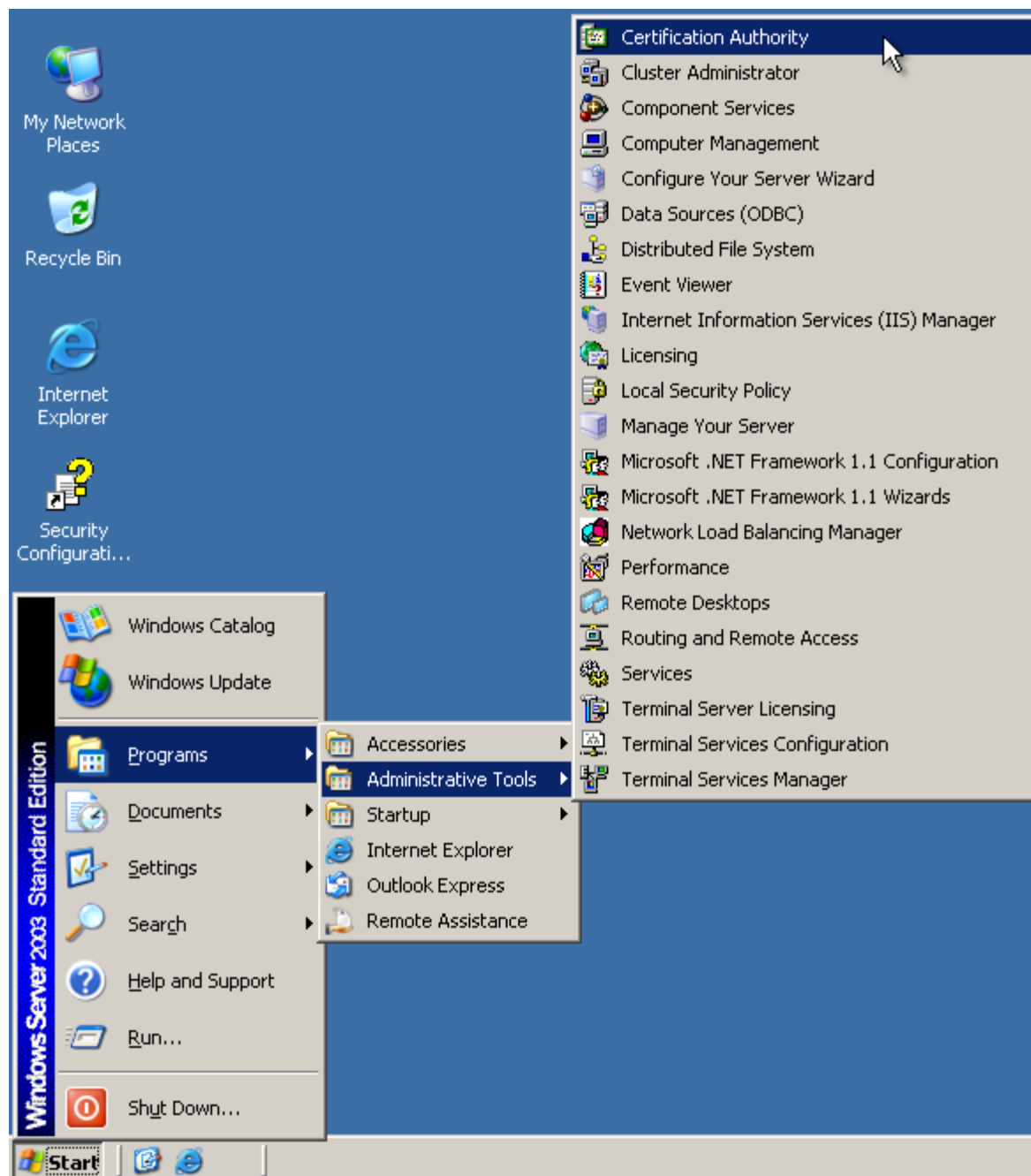


- Điền các thông số name và suffix tương tự như sau:

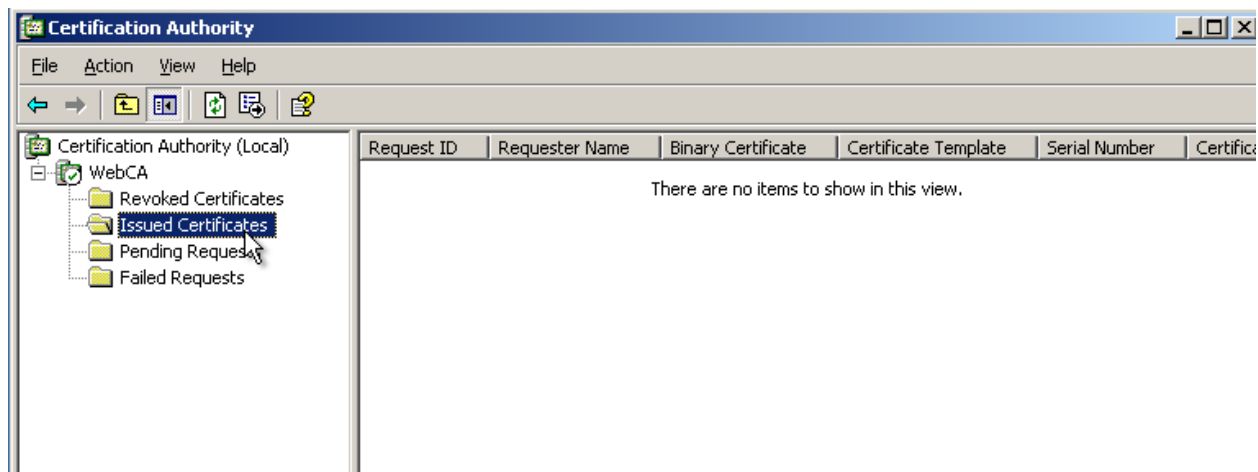


- Cài đặt thêm component ASP:



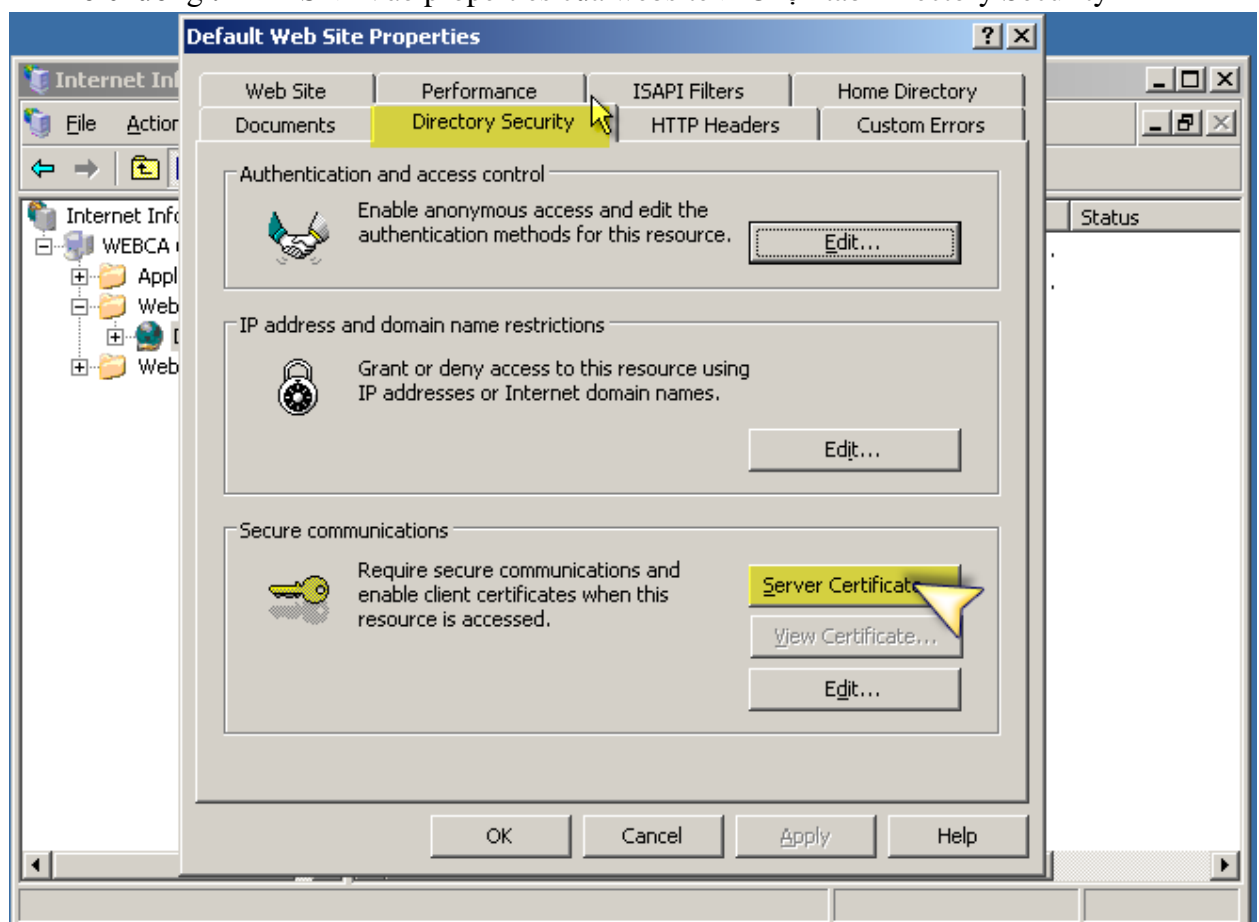


- Mở chương trình Certificate Authority để kiểm tra việc cài đặt:
 - + Revoke Certificates: các certificates hết hạn sử dụng bị thu hồi
 - + Issued Certificates: các certificate đã cấp phát
 - + Pending Certificate: các certificate đã được yêu cầu, đang đợi cấp phát
 - + Failed Certificates: các certificate sau quá trình pending nhưng cấp phát không thành công



B. Cấu hình sử dụng certificate để chứng thực cho website:

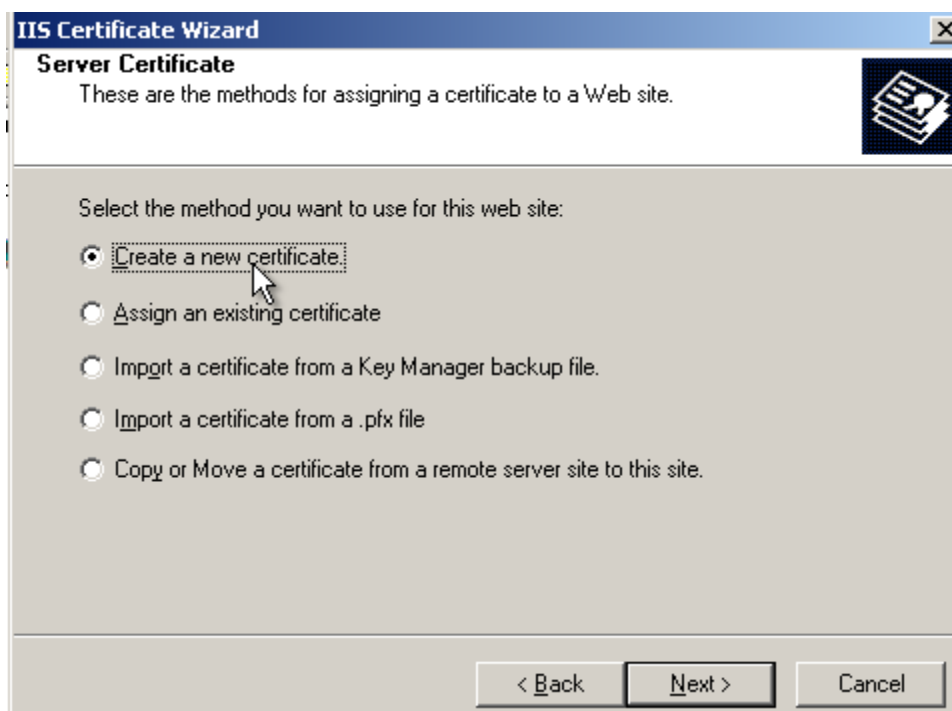
- Mở chương trình IIS -> Vào properties của website-> Chọn tab Directory Security



- Thực hiện request 1 certificate:



- Chọn yêu cầu một certificate mới cho website:



IIS Certificate Wizard

Delayed or Immediate Request

You can prepare a request to be sent later, or you can send one immediately.

Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

☒ Prepare the request now, but send it later

☐ Send the request immediately to an online certification authority

< Back Next > Cancel

IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

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

Name:

Default Web Site

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: 1024

☐ Select cryptographic service provider (CSP) for this certificate

< Back Next > Cancel

IIS Certificate Wizard [X]

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

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:
WebCA

Organizational unit:
WebCA

< Back Next > Cancel

IIS Certificate Wizard [X]

Your Site's Common Name

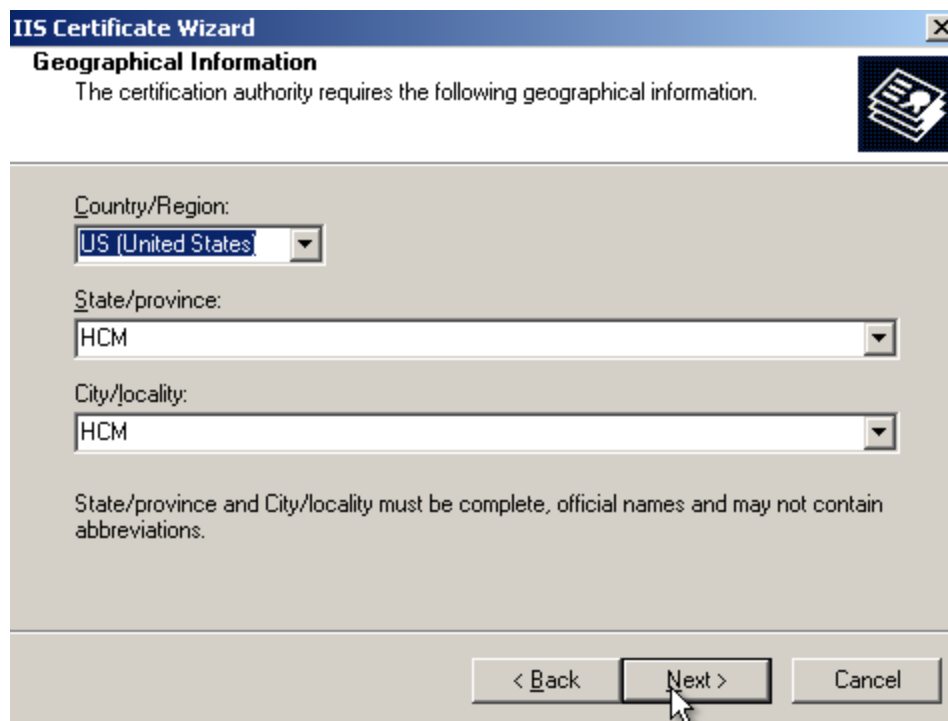
Your Web site's common name is its fully qualified domain name.

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:
webca

< Back Next > Cancel



IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

Country/Region:
US (United States)

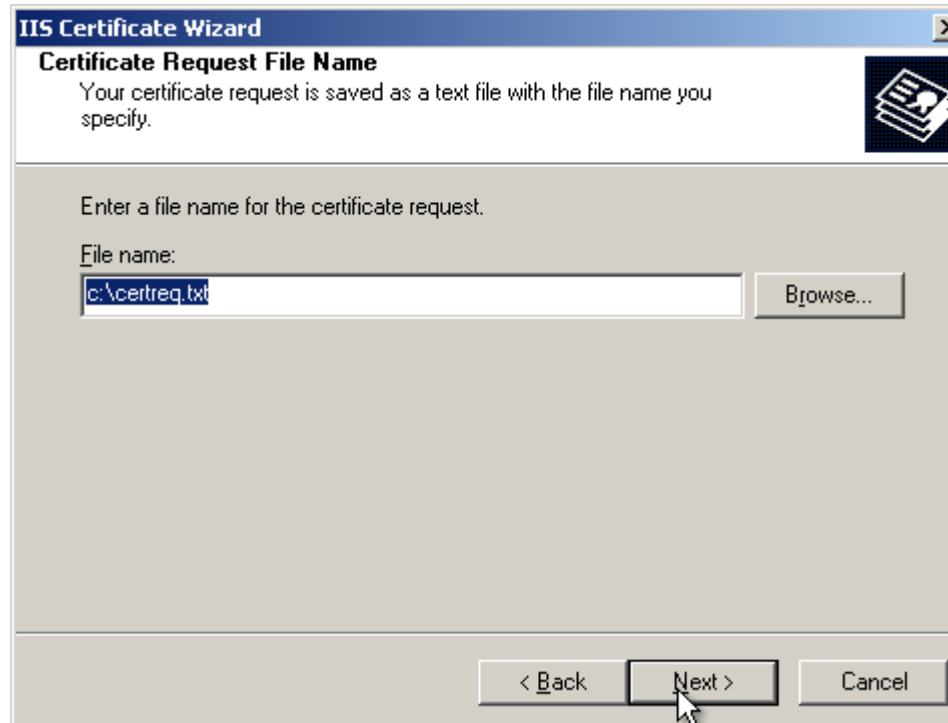
State/province:
HCM

City/locality:
HCM

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

< Back Next > Cancel

- Chọn nơi lưu trữ file certificate request:



IIS Certificate Wizard

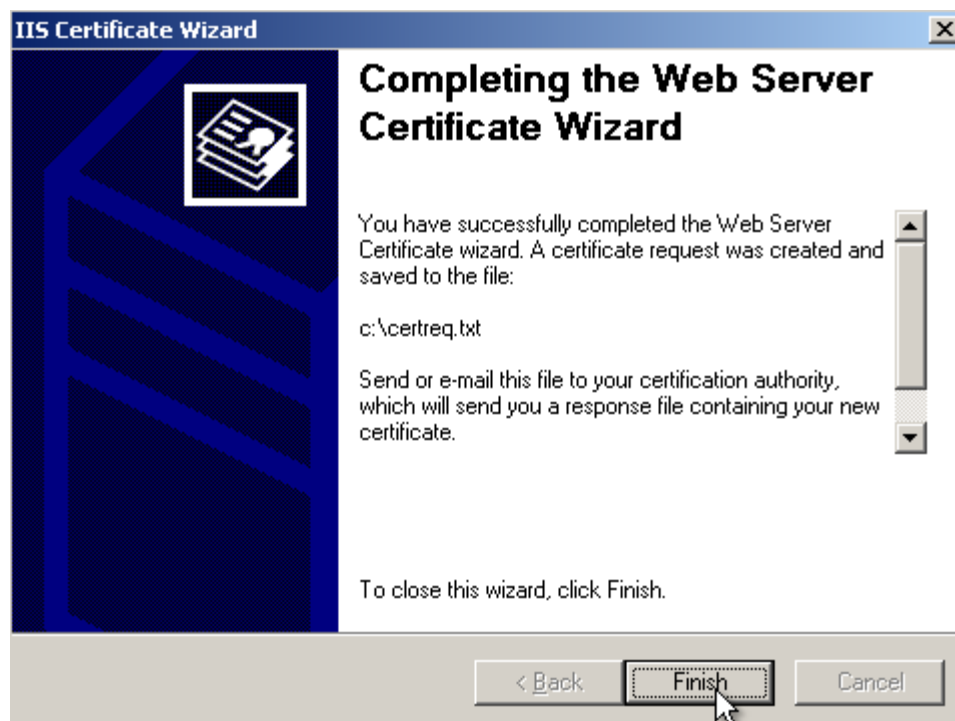
Certificate Request File Name

Your certificate request is saved as a text file with the file name you specify.

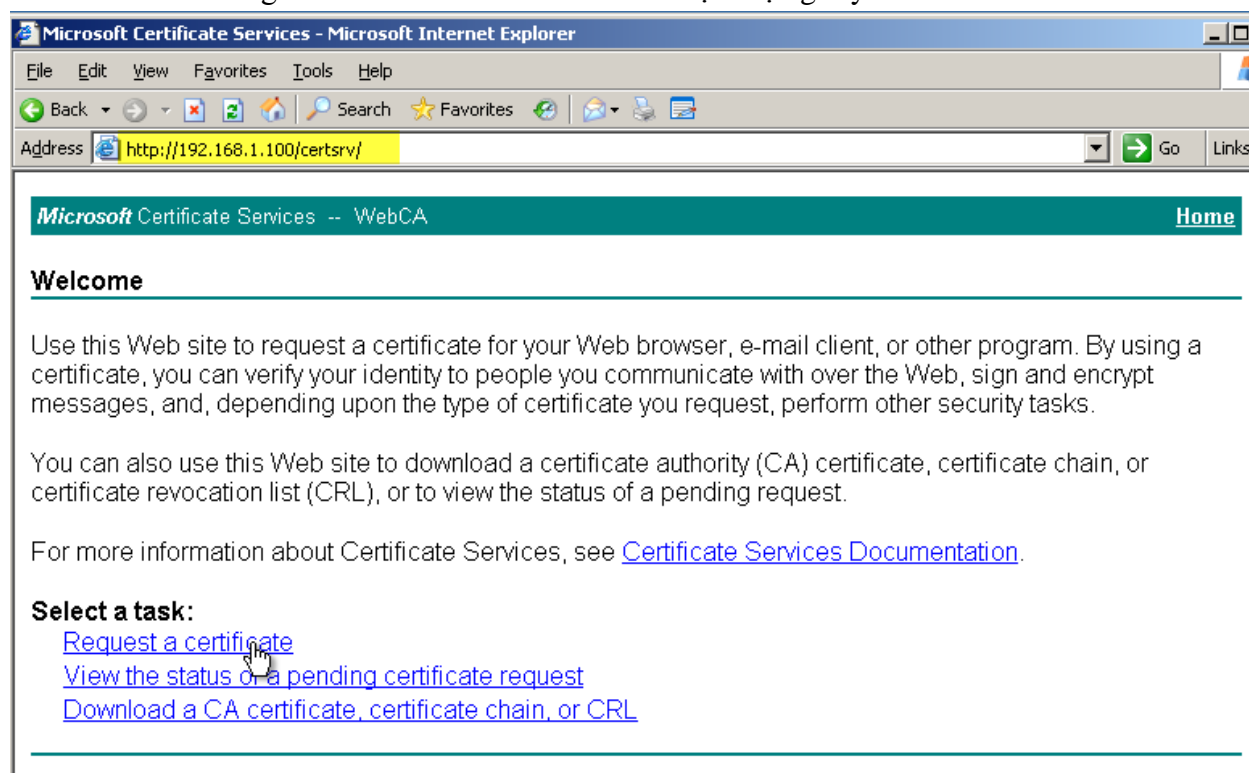
Enter a file name for the certificate request.

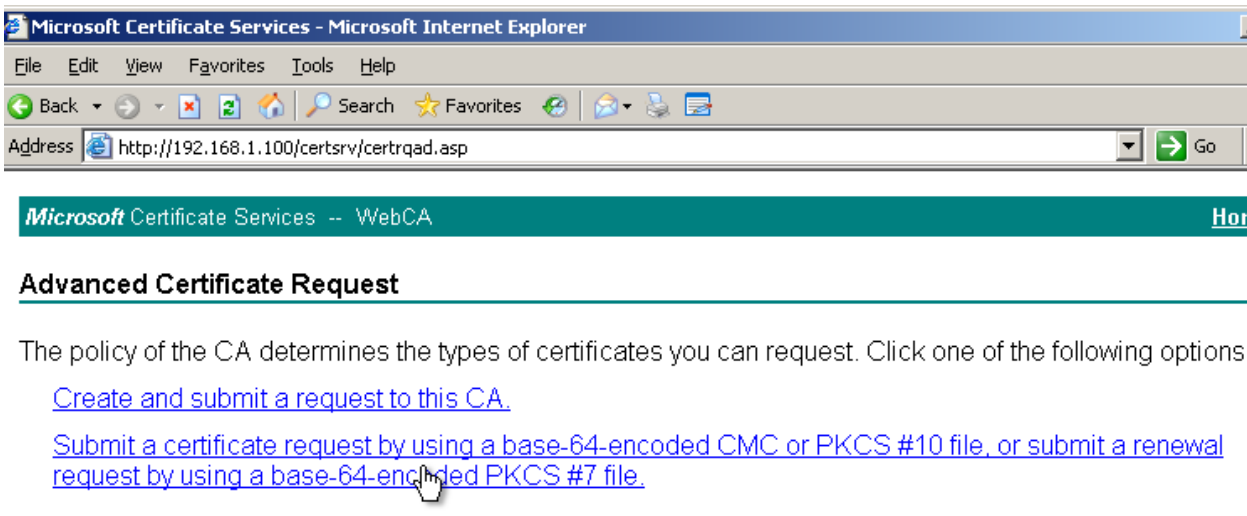
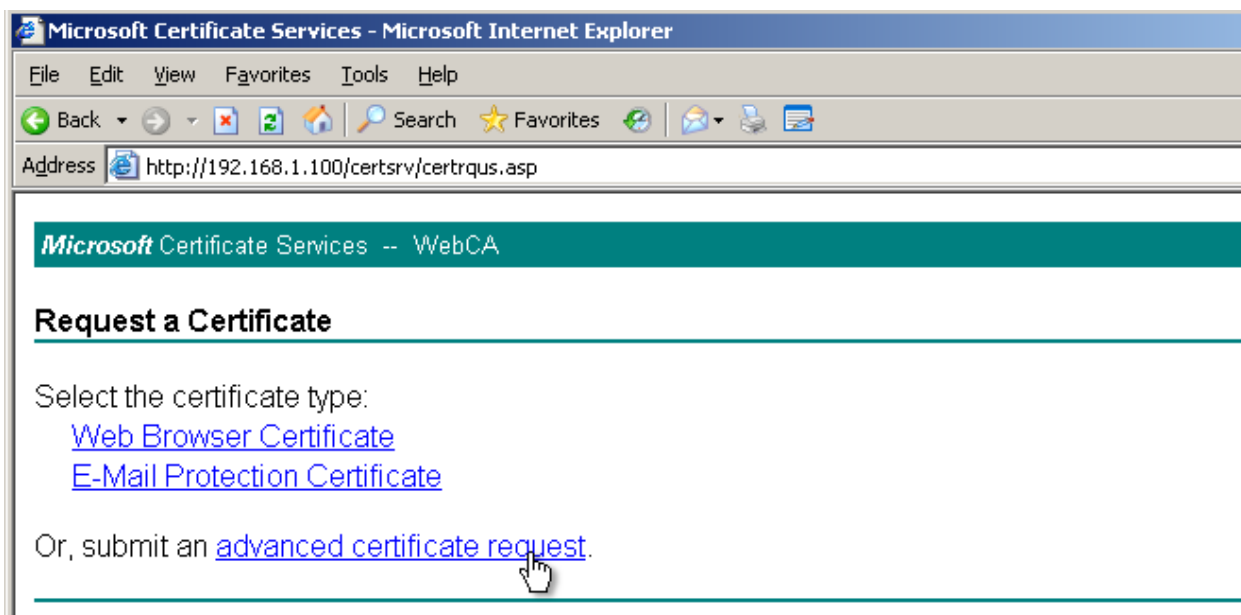
File name:
c:\certreq.txt Browse...

< Back Next > Cancel



- Vào trang web 192.168.1.100/certsrv để thực hiện gửi yêu cầu đến CA server:





- Browse đến file certreq.txt đã lưu hoặc copy nội dung file này paste vào khung màu vàng:

Microsoft Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Mail Print

Address <http://192.168.1.100/certsrv/certrqxt.asp> Go Links >>

Microsoft Certificate Services -- WebCA [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
AAAAAAAAAwDQYJKoZIhvcNAQEFBQADgYEAsi8ySiA7EpdMBko3T68019932b6usfXVJvTcT6bHeyMfvoELZ7Xg5gWdR7L2Nmci+O1Yrv8/6uINjeEh6GmPgrcpvD1HxLySKo=-----END NEW CERTIFICATE REQUEST-----
```

[Browse for a file to insert.](#)

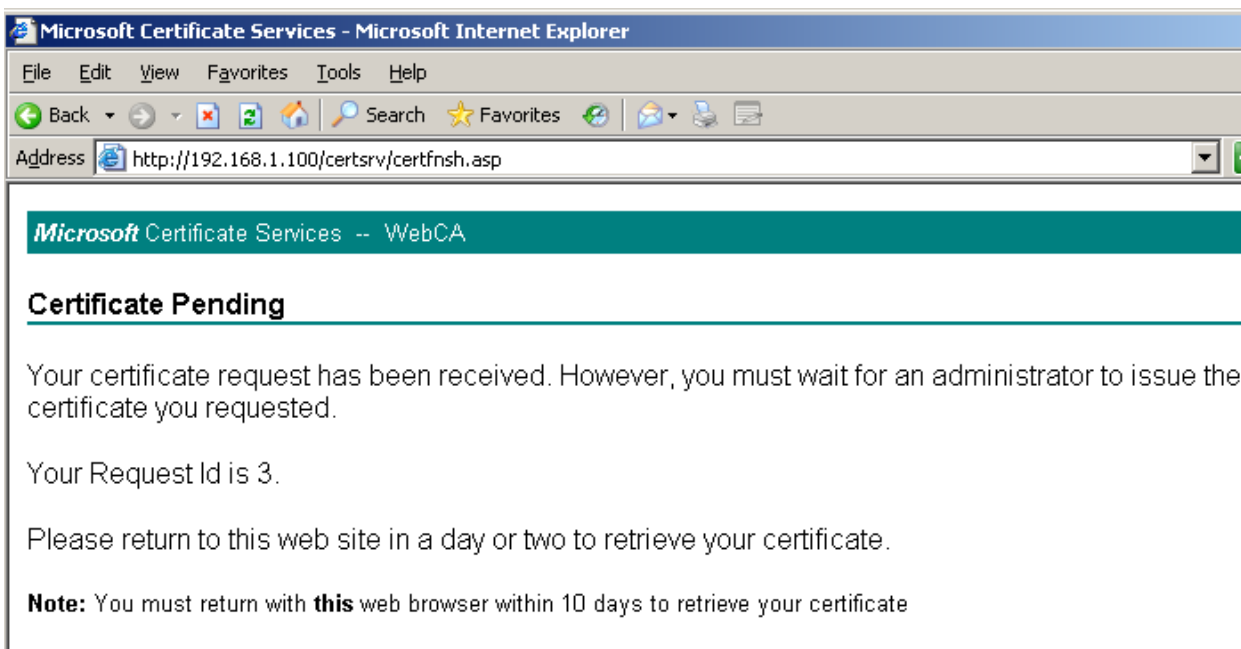
Additional Attributes:

Attributes:

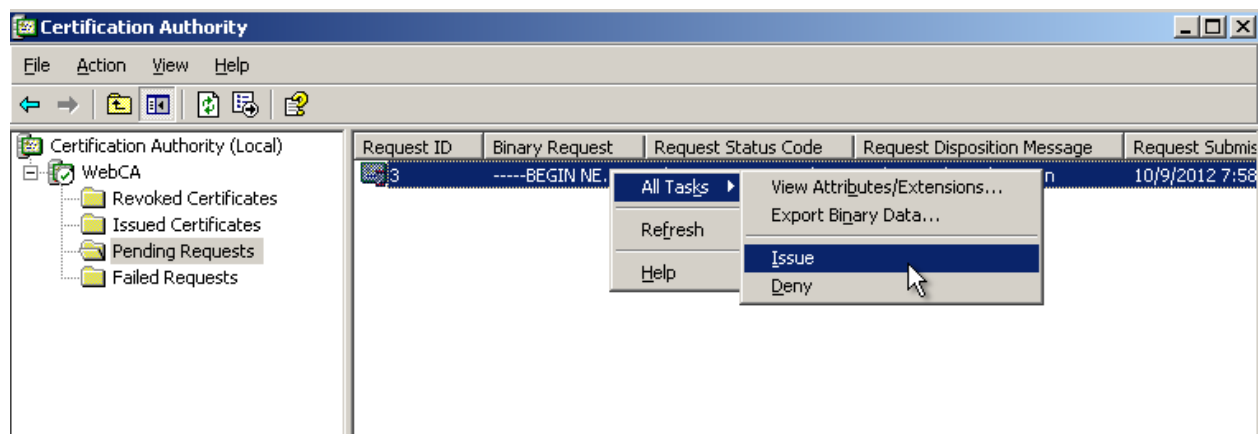
Submit

Trusted sites

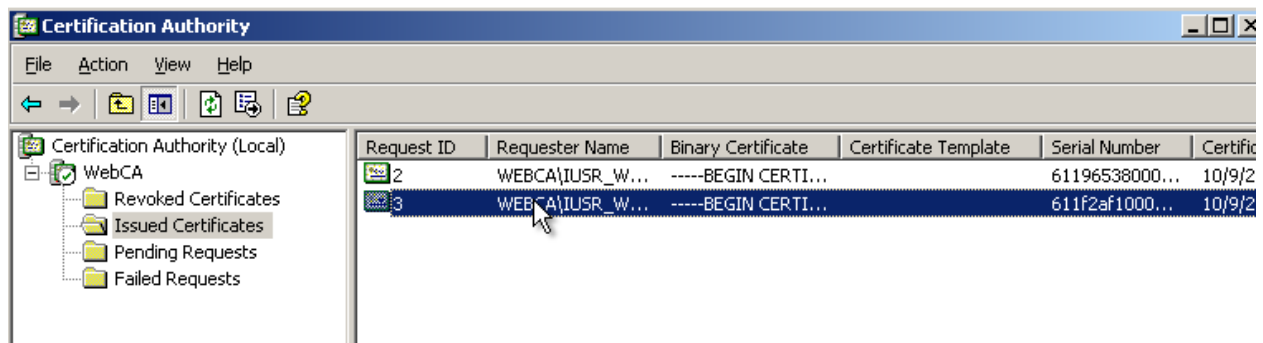
- Sau khi yêu cầu thành công, certificate được đưa vào quá trình chờ cấp phát:



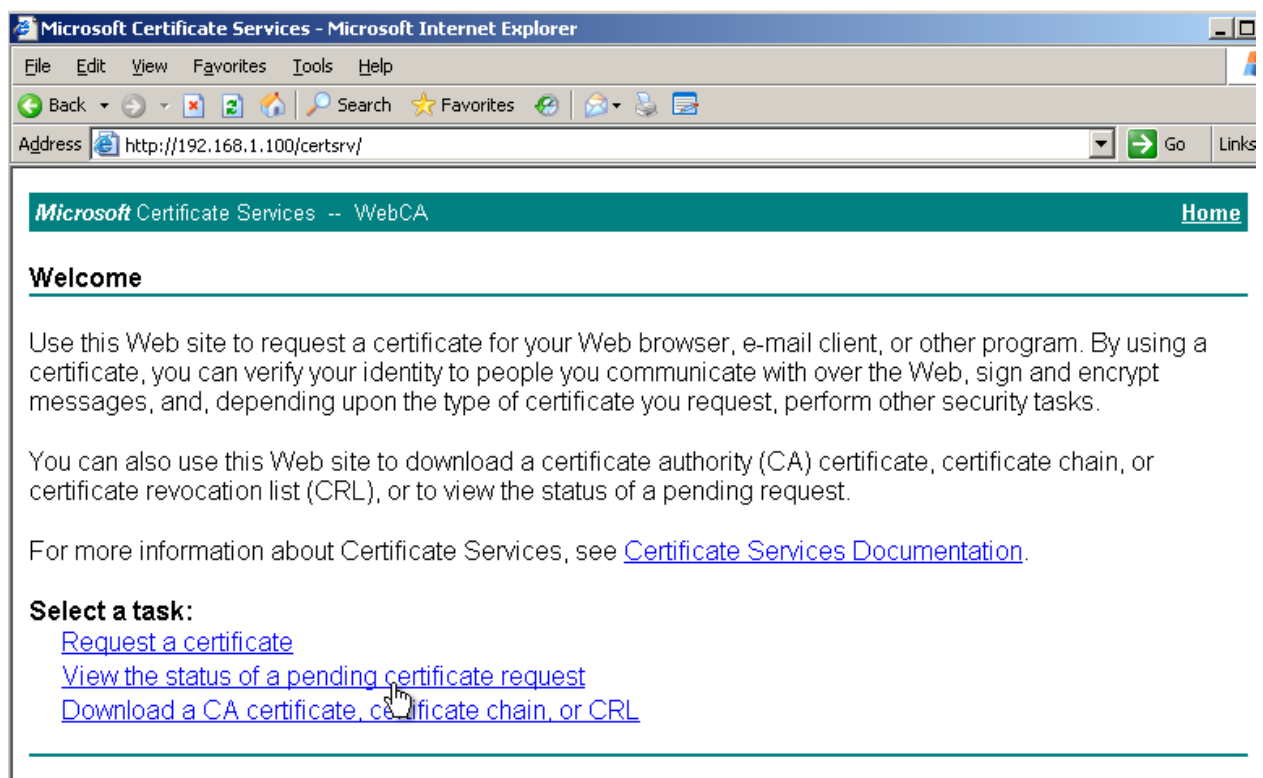
- Mở chương trình Certification Authority: thực hiện cấp phát ngay CA cho website thay vì đợi sau khoảng thời gian mặc định:

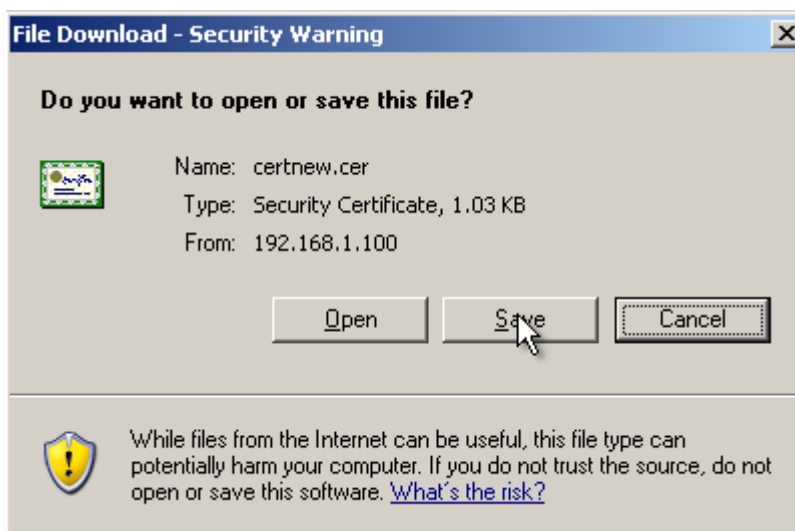
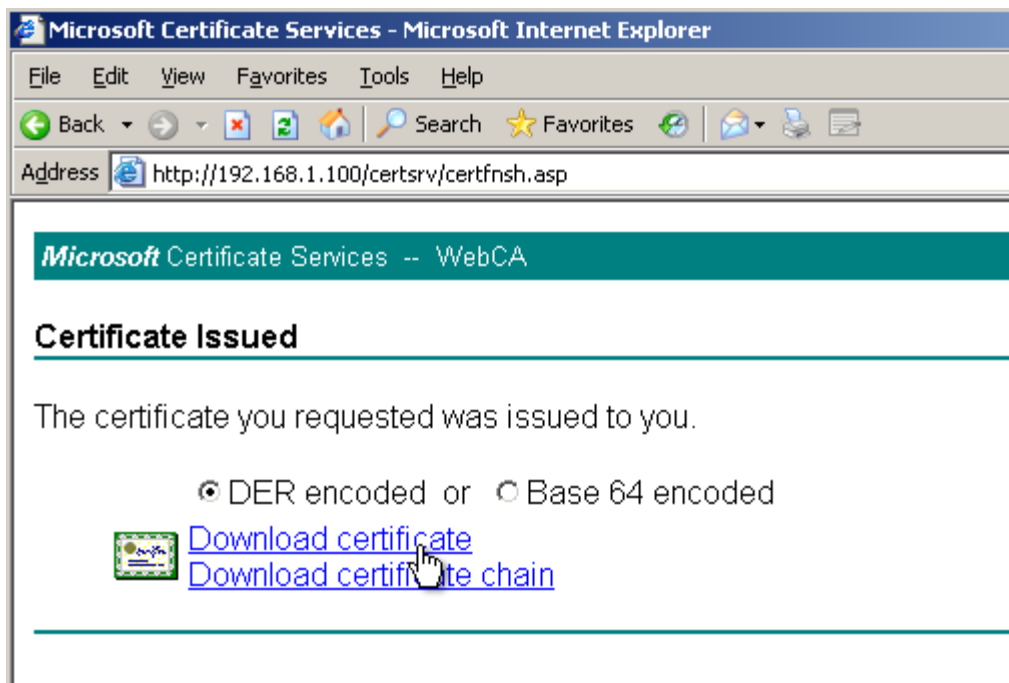


- Kết quả sau khi cấp phát:

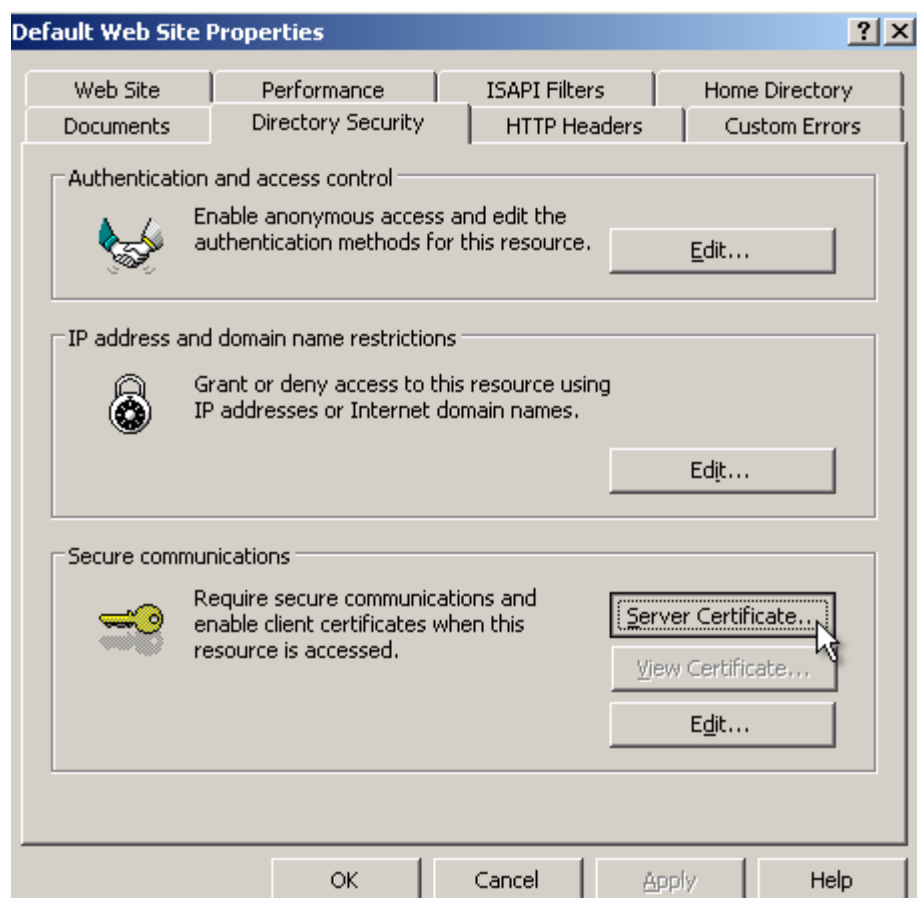


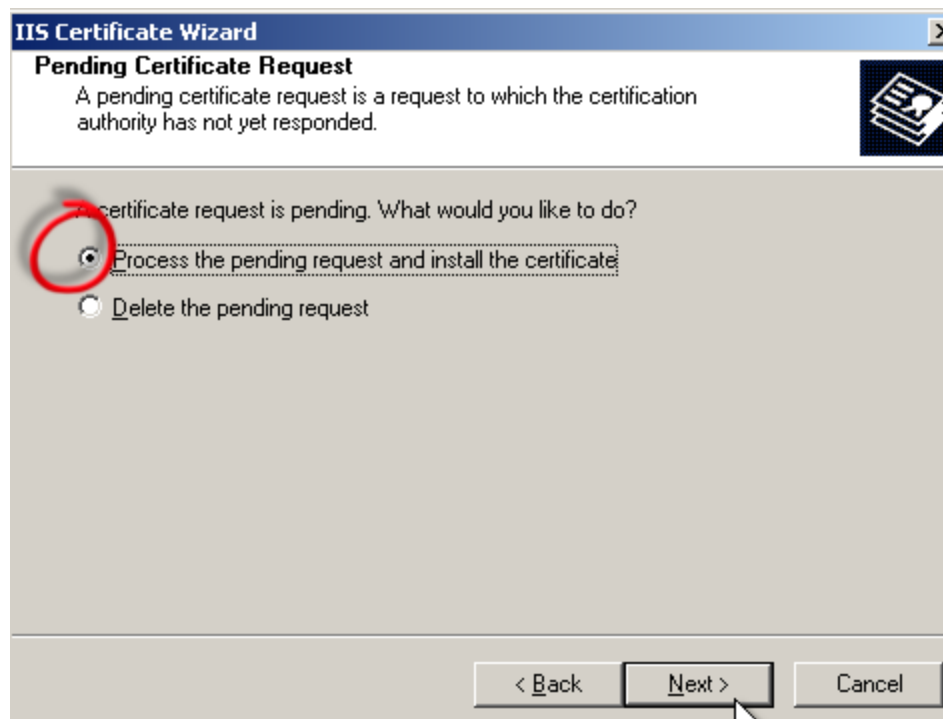
- Tiến hành download certificate về máy tính làm web server:



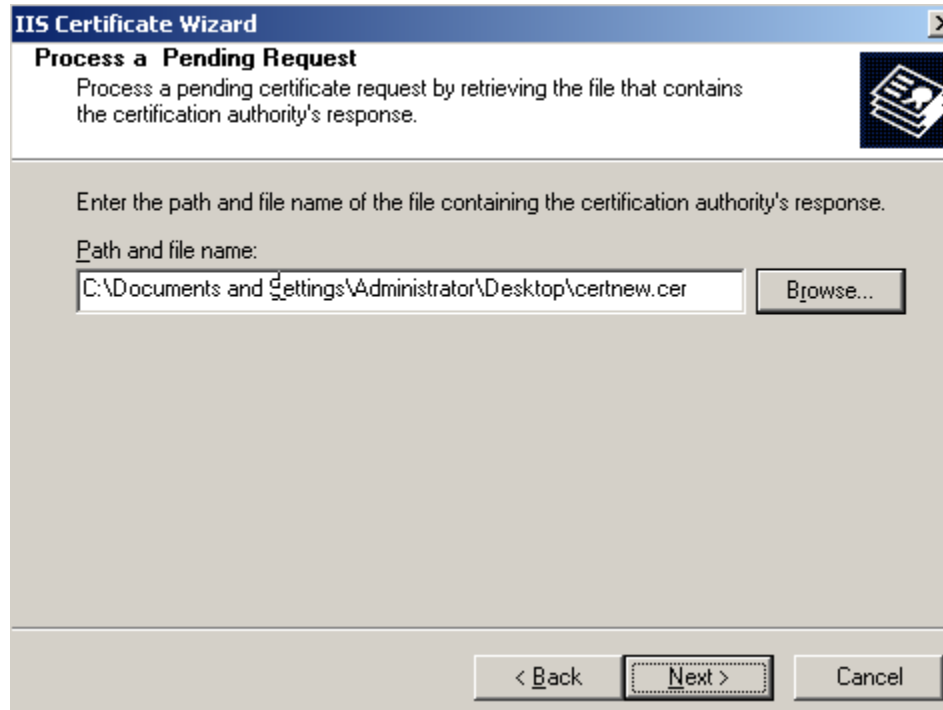


- Mở chương trình IIS: thực hiện cài đặt certificate vừa download về:

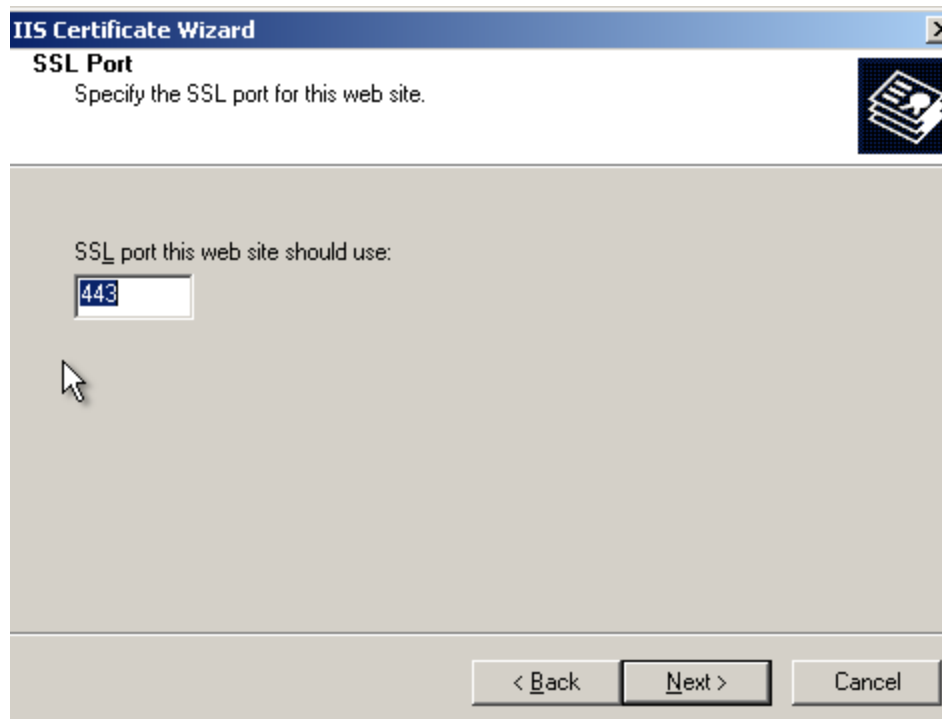




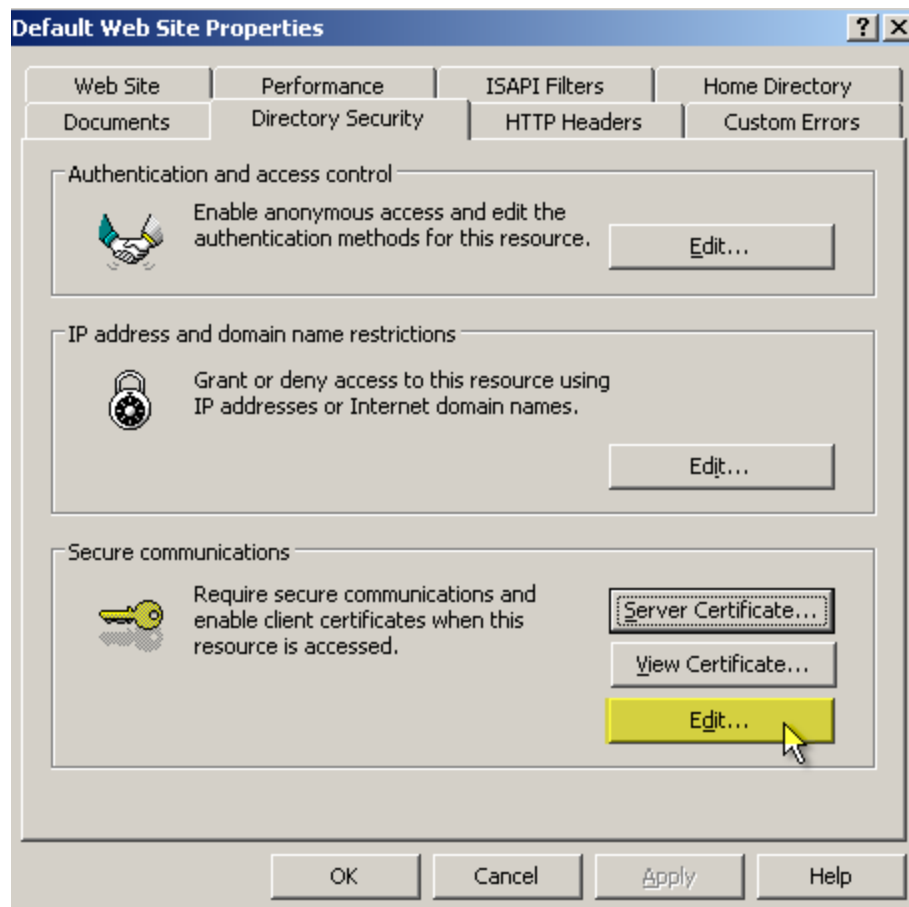
- Browse đến file certificate vừa download:

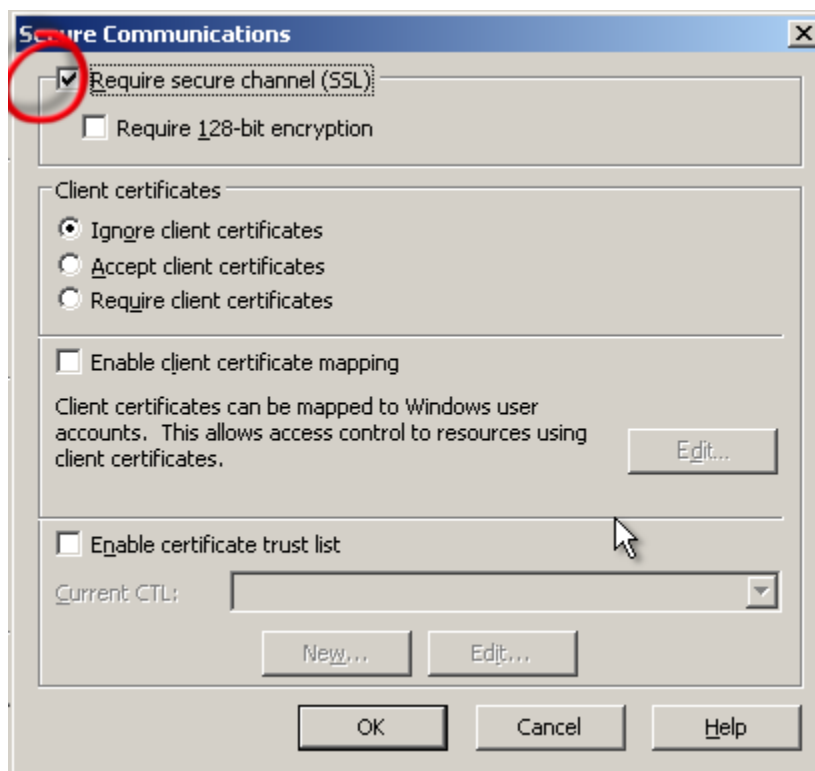


- Để mặc định port sử dụng cho trang web là 443 (dùng giao thức SSL)



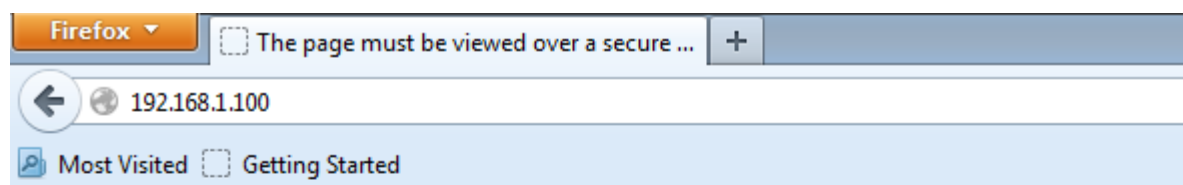
- Sau khi cài đặt hoàn tất, ta trở lại cửa sổ properties của website, thiết lập yêu cầu dùng giao thức SSL để truy cập website:





C. Kiểm tra:

- Từ máy tính khác truy cập vào website qua địa chỉ: <http://192.168.1.100> không thành công:



The page must be viewed over a secure channel

The page you are trying to access is secured with Secure Sockets Layer (SSL).

Please try the following:

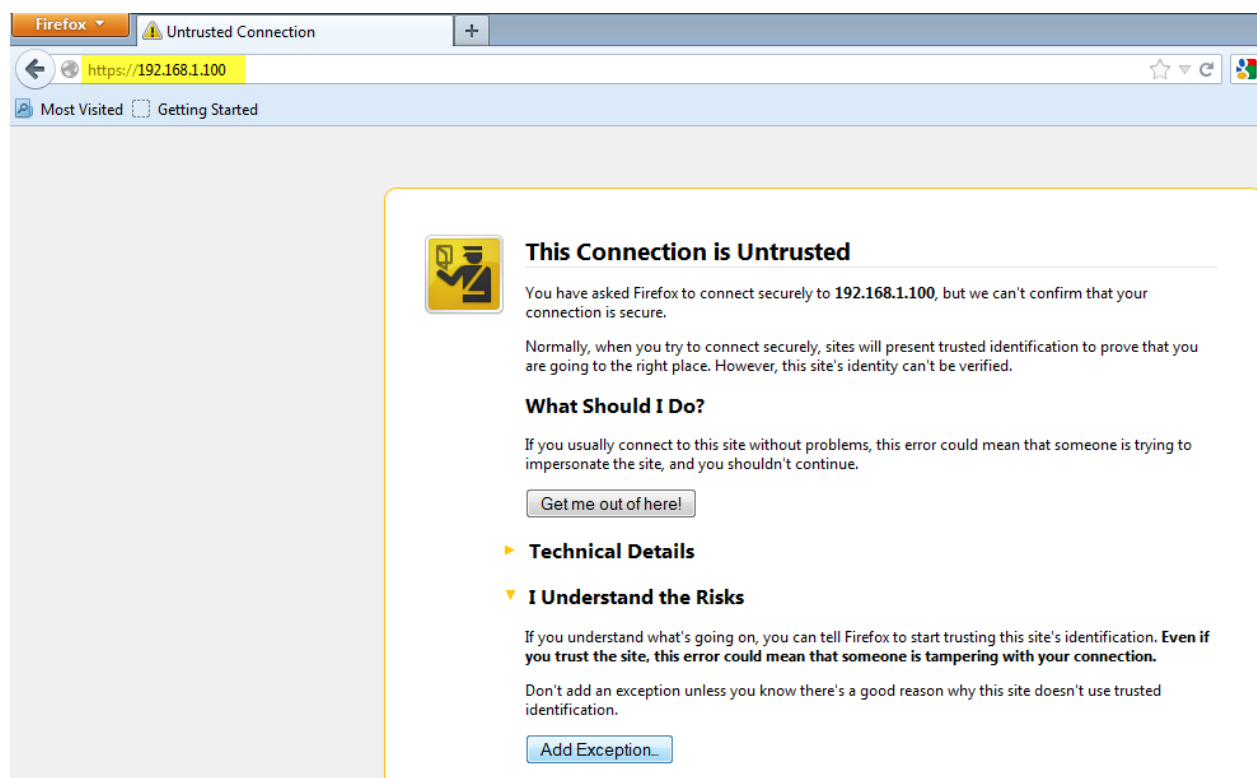
- Type **https://** at the beginning of the address you are attempting to reach and press ENTER.

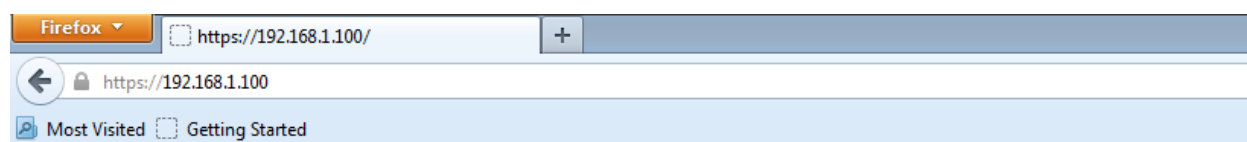
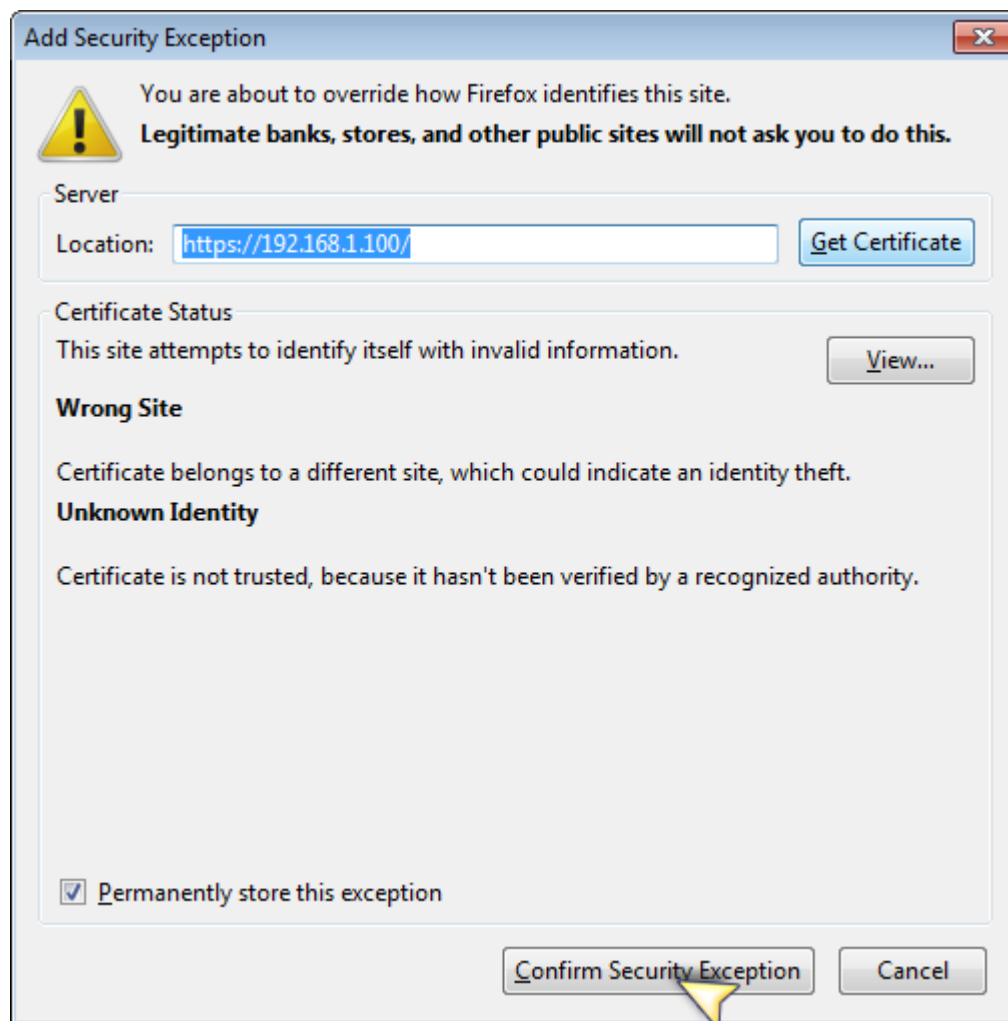
HTTP Error 403.4 - Forbidden: SSL is required to view this resource.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to [Microsoft Product Support Services](#) and perform a title search for the words **HTTP** and **403**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **About Security**, **Secure Sockets Layer (SSL)**, and **About Custom Error Messages**.

- Truy cập lại với địa chỉ <https://192.168.100>. Trình duyệt yêu cầu accept certificate:





Website TKUDM