**What are self signed certificates**  
A self-signed certificate is an identity certificate that is signed by its own creator. Certificates are signed by Certificate Authority. In general self signed certificates are fine for testing purposes and not for production use.  
  
**Creating self-signed certificates**  
There are several ways to create self signed test certificates. Let us explore 2 of the easier options available. The easiest and simpler approach is to use IIS to create these certificates. In IIS 7.5  
**1.** Click on the "Server Name"  
**2.** Double click "Server Certificates" feature  
**3.** Click on "Create Self Signed Certificate" link, under "Actions"  
**4.** Specify a friendly name for the certificate and click OK. The friendly name is not part of the certificate itself, but is used by the server administrator to easily distinguish the certificate.   
  
   
  
**The generated test certificate, is also automatically installed into the certificate store.**  
  
**MakeCert.exe** tool can be used as another way to generate, test certificates. The following link from microsoft explains, various options that can be used with this tool. This is a command line tool and must be run from visual studio command prompt.   
http://msdn.microsoft.com/en-us/library/bfsktky3.aspx  
  
**Makecert** -r -pe -n "CN=YourComputerName" -b 01/01/2000 -e 01/01/2100 -ss my -sr localMachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12  
  
**Note:** Replace YourComputerName, with the name of your computer.  
  
**Associating an asp.net web application with a specific certificate**  
Add HTTPS site binding, if it is not already present  
1. Open IIS  
2. Expand the "Server Name"  
3. Expand "Sites"  
4. Select "Default Web Site"  
5. Click "Binding" under "Edit Site" in "Actions" pane.  
6. In the "Site Bindings" window, Click "Add"  
7. Select Type = "https" and the SSL Certificate and click "OK"  
8. Click "Close" on "Site Bindings" window  
  
At this point, you will be able to access your application using both HTTP and HTTPS protocol. When the site is accessed over HTTPS, you may receive a browser warning about the authenticity of the website. In a later video session we will discuss about resolving this.  
  
**If you want to dis-allow, access over HTTP protocol there are 2 ways**  
**First Way:** Remove HTTP binding at the IIS Server level. This option will prevent all the web applications, running on that server to use only HTTPS binding.   
  
**Second Way:** Let both the bindings be available at the server level and configure SSL settings at an application or web site level.   
1. Select your web application in IIS  
2. Double click "SSL Settings" from the features window  
3. Make sure "Require SSL" check box is checked.  
4. Click "Apply" under "Actions" pane  
  
Now, if you try to access the application using HTTP instead of HTTPS, you will get an error