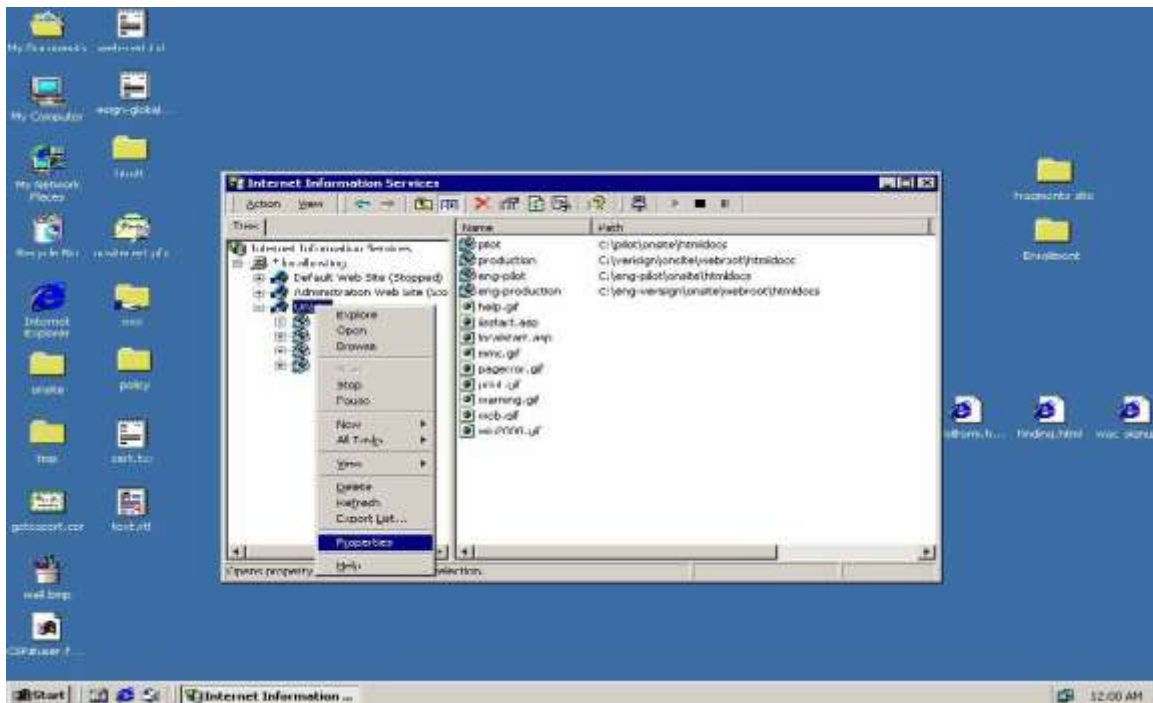
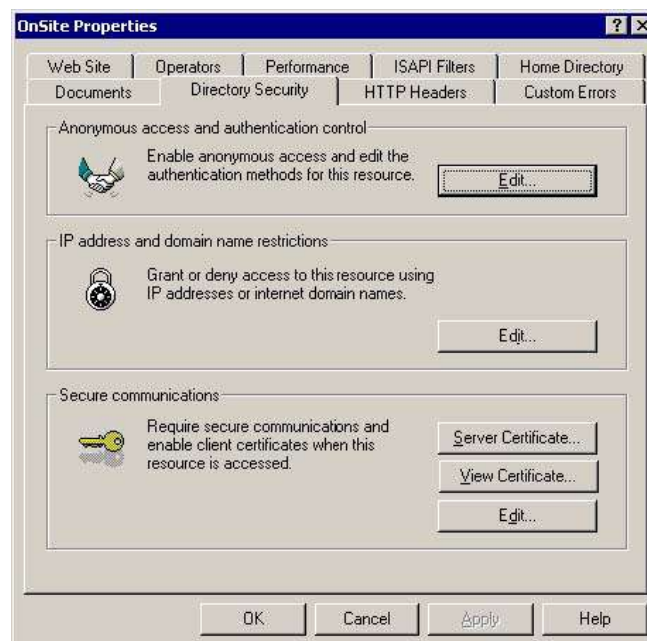


Configuring options for server authentication using digital certificates (IIS)

From Start\Programs\Administrative Tools select the option Internet Information Server. Select the web site on which a server certificates is installed and you want to perform authentication with certificates. Right-click and select the Properties option...



From the following window select the tab Directory Security and press the button Edit in that window... from the Secure communications sections.

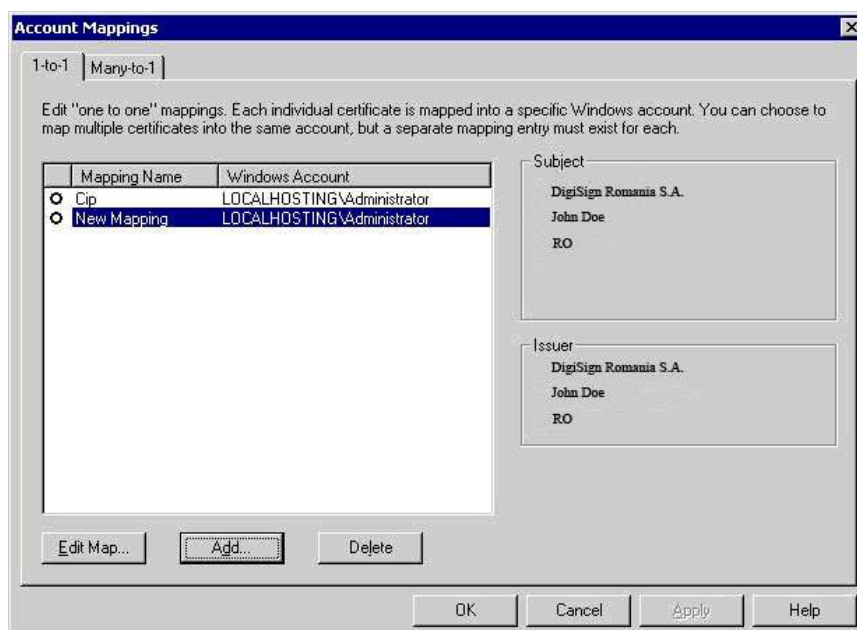


Check the boxes “Require secure channel (SSL)”, “Enable client certificate mapping” and “Enable certificate trust list”.



In Client certificates you may choose one of the variants. If you choose “Accept client certificates”, authentication can be made both based on digital certificates and based on user and password. If you choose „Require client certificates”, can only be made by digital certificates.

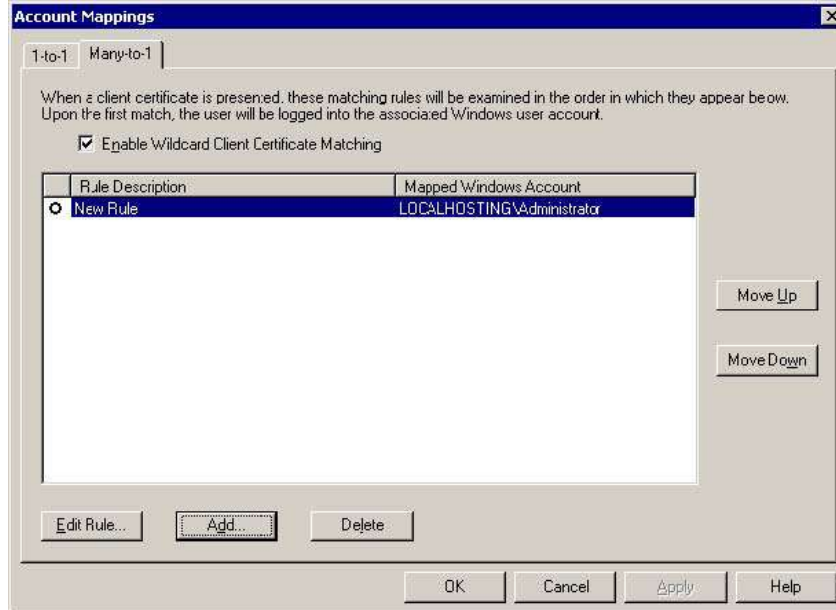
In “Enable client certificate mapping” section, press the button Edit. You may choose in this stage one of the accounts mapping options. It can be “1-to-1” (one digital certificate is mapped to each account) or “Many-to-1” (one certificate in mapped for multiple accounts).



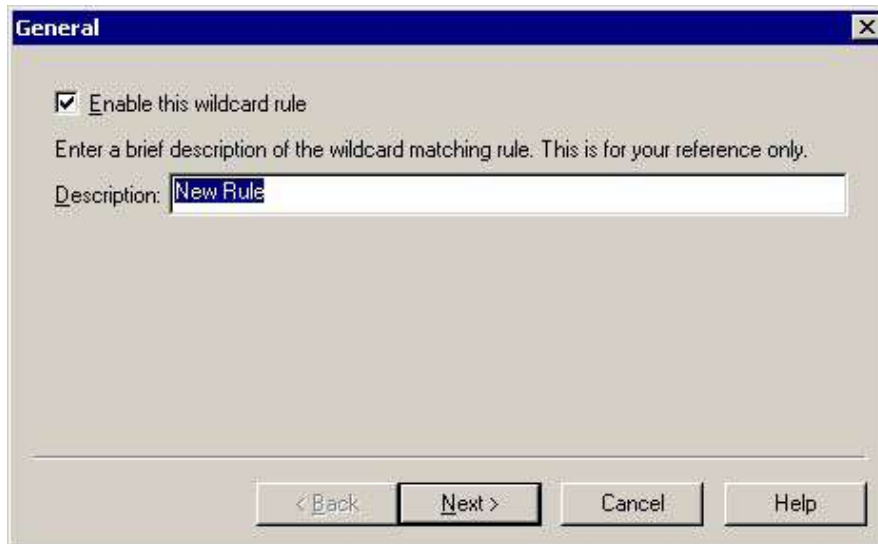
If you have chosen “1-to-1”, press the button Add., enter user name (of that account) and attach a valid digital certificate to it. That certificate is to be found as a file having the extension .cer and contains the public key.



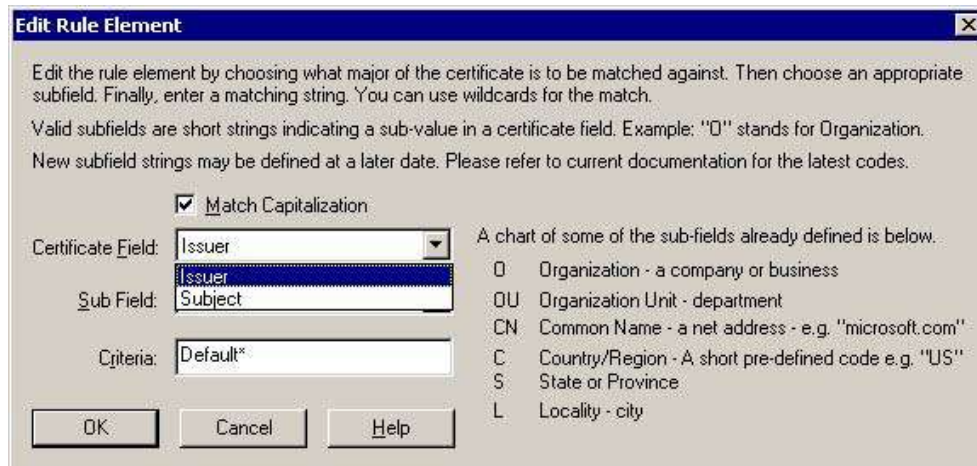
If you have chosen the mapping “Many-to-1”, a rule is created for authentication with digital certificates. Press the button Add...



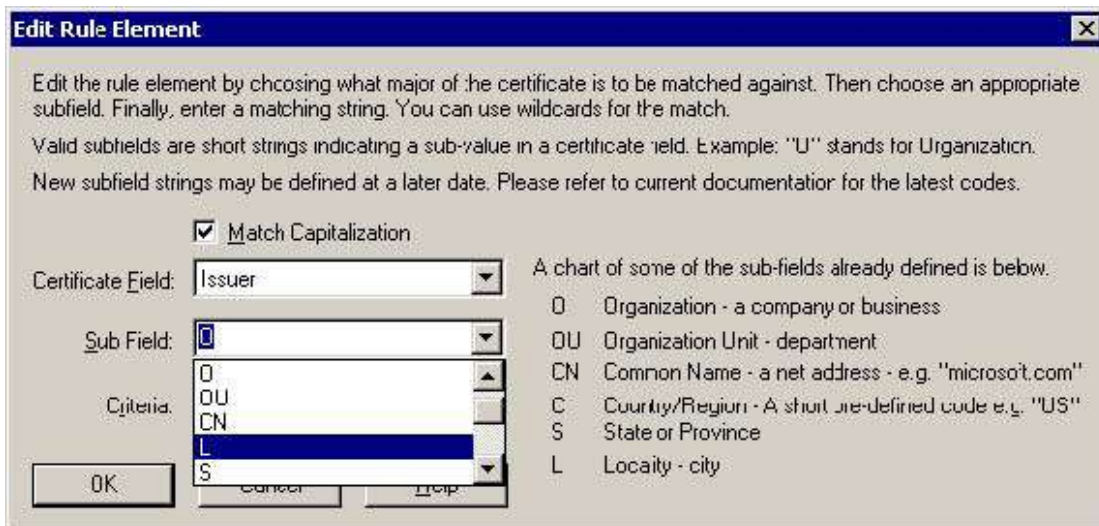
Select a friendly name for this rule and then press the button Next. Under Rules window, press New in order to create a new mapping rule.



You reach a window “Edit Rule Element” where you can select the criteria on which you want to make authentication with certificates. The authentication can be made by issuer or by certain sub-fields from the field Subject. This information is comprised by each certificate.



For the field Sub Field you may select one of the variants below, where O is the company issuing these certificates (here DIGISIGN S.A.), OU represents the Organization Unit, CN represents a Common Name, E represents the e-mail address. You may find all the information on certificates in the section Details \ Subject.



After establishing the criteria, press the button OK and you will be prompted to select one of the options below. Select the option "Accept this certificate for Logon Authentication" and select the account (accounts) to which this rule is matched.



Then press the button Finish.

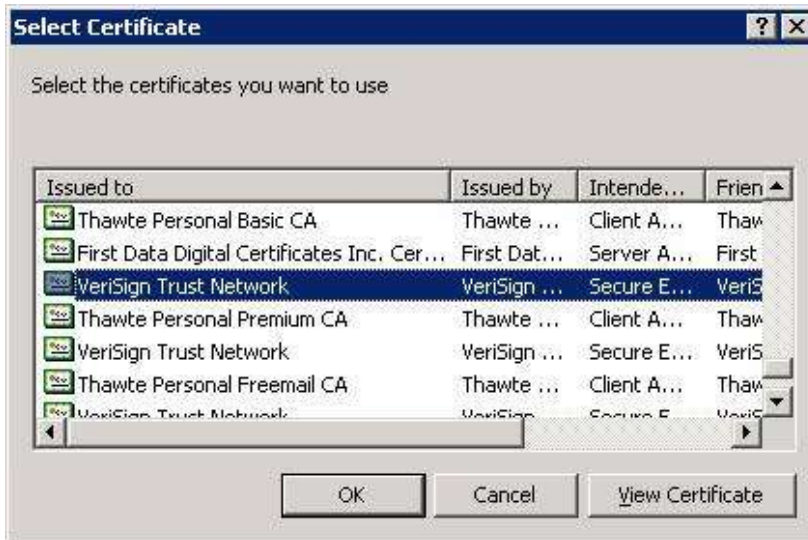
In order to configure the option “Enable certificate trust list” press the button Edit.



Press the button Next and the window “Certificates in the CTL” will be displayed. In order to select the certification authority’s certificates press the button Add from Store (you can import them directly from browser) or Add from File (make the import from the files with the extension .cer downloaded from the web site).



Then press the button Next. Select the certification authority’s certificate (in this case VERISIGN TRUSTED NETWORK) and then press the button OK.



Give a friendly name to this option and press the button Next.
In order to complete this wizard, press the button Finish.

