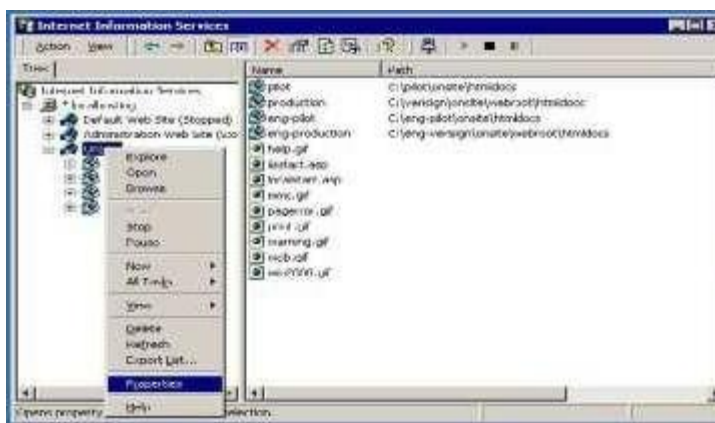
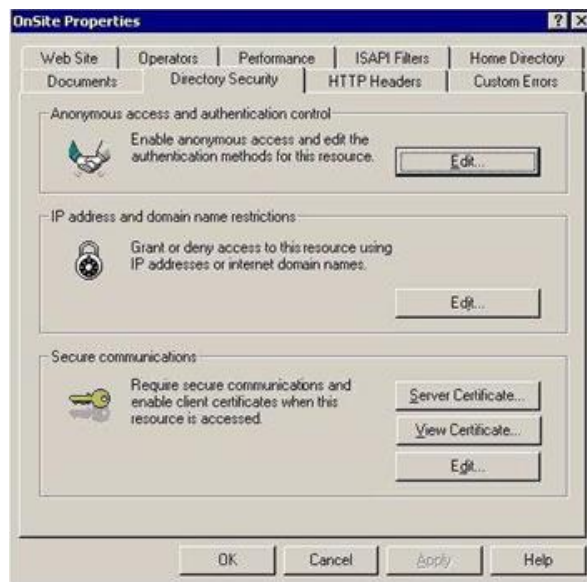


Configurarea opțiunilor pentru autentificarea pe server utilizând certificatele digitale (IIS)

1. Selectați meniul Start ⇒ Programs ⇒ Administrative Tools ⇒ Internet Information Services. Selectați site-ul web pe care aveți instalat un certificat de server și pentru care doriți să realizați autentificarea cu ajutorul certificatelor digitale. Selectați opțiunea **Properties** prin *click-dreapta*.



2. Alegeți tab-ul **Directory Security** și din secțiunea **Secure communications** apăsați butonul **Edit**.

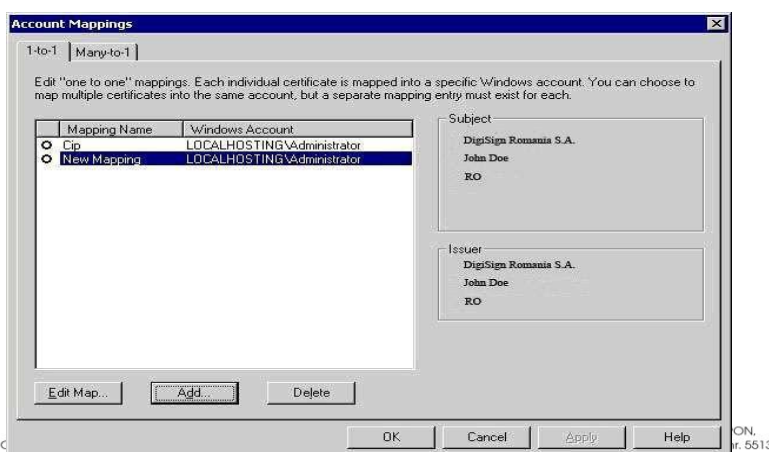


3. Bifați căsuțele “Require secure channel (SSL)”, “Enable client certificate mapping” și “Enable certificate trust list”.

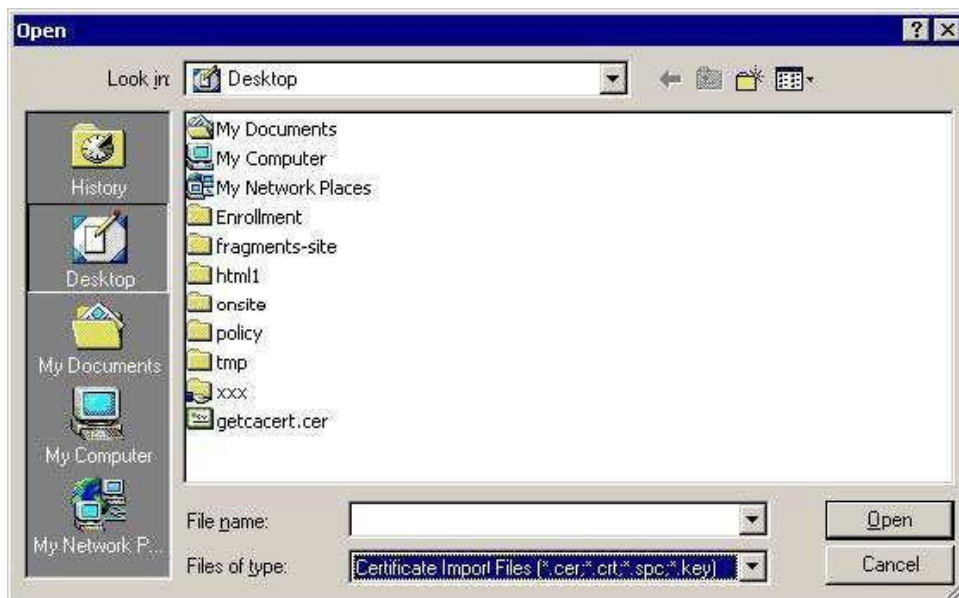


În secțiunea **Client certificates** puteți opta pentru una din variante. În cazul în care alegeți varianta “Accept client certificates”, autentificarea se poate realiza atât pe bază de certificate digitale cât și pe bază de user și parolă. Dacă optați pentru “Require client certificates”, autentificarea se realizează numai pe bază de certificate digitale.

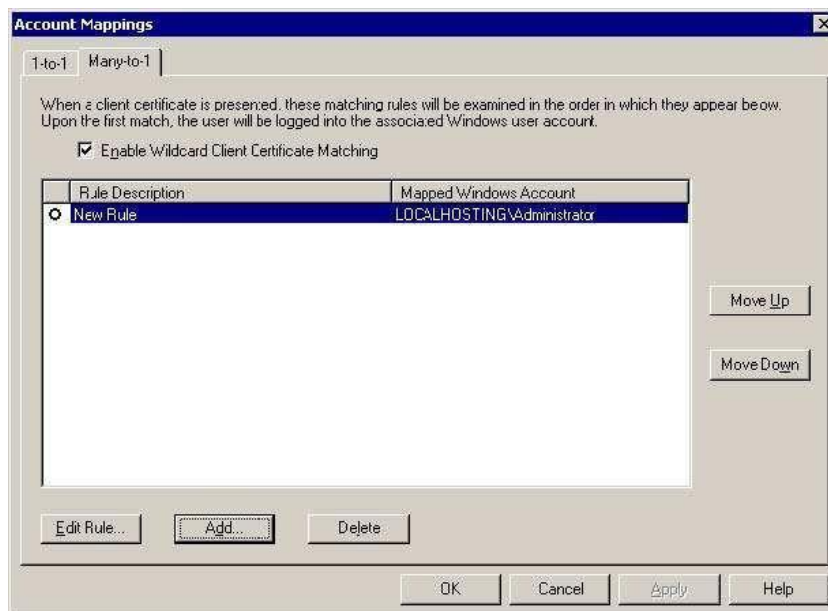
În secțiunea “Enable client certificate mapping” apăsați butonul Edit. În această etapă puteți opta pentru una din opțiunile de mapare a conturilor. Poate fi “1-to-1” (fiecărui cont i se atribuie un certificat digital) sau “Many-to-1” (se atribuie un singur certificat pentru mai multe conturi).



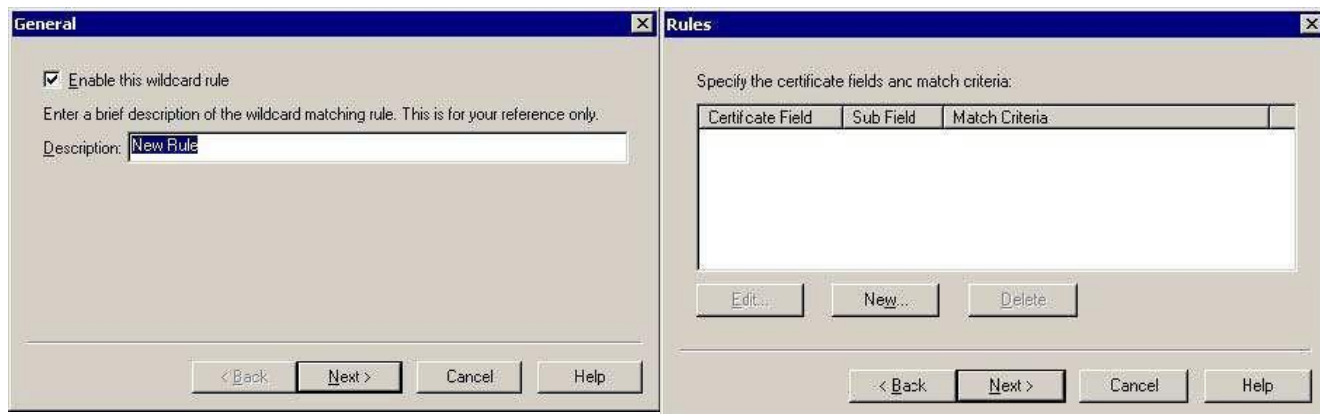
În cazul în care ați ales opțiunea “1-to-1”, apăsați butonul **Add**, introduceți numele userului (contului respectiv) și atașați-i un certificat digital valid. Certificatul respectiv se găsește sub forma unui fișier cu extensia .cer și conține cheia publică.



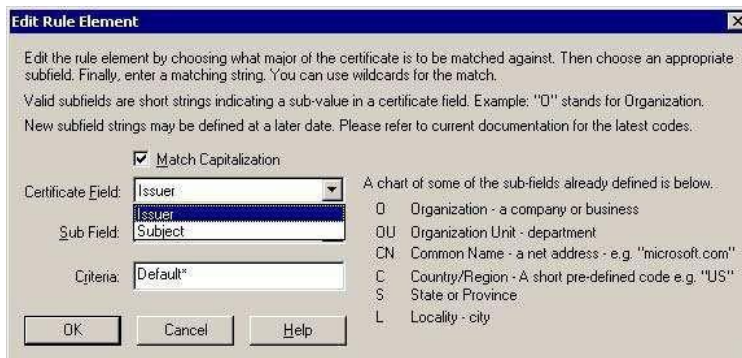
În cazul în care optați pentru atribuirea “Many-to-1”, se creează o regulă pentru autentificarea cu certificate digitale. Apăsați butonul **Add**.



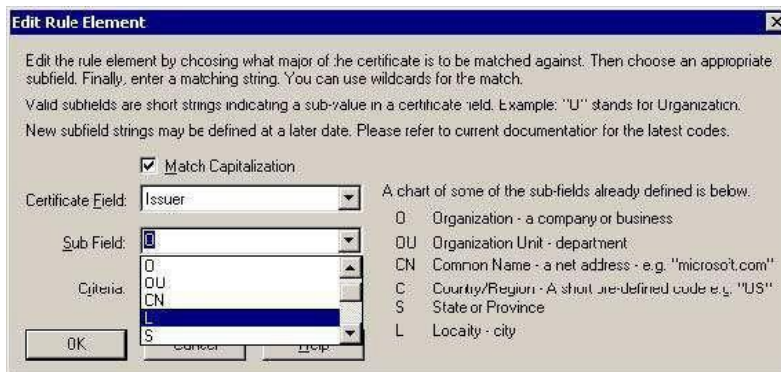
Alegeți un nume sugestiv pentru această regulă și apăsați apoi butonul **Next**. În fereastra **Rules**, apăsați butonul **New** pentru a crea o nouă regulă de mapare.



Veți ajunge într-o fereastră "Edit Rule Element" unde vă puteți alege criteriile după care doriți să realizați autentificarea cu ajutorul certificatelor. Autentificarea se poate realiza după emitent (Issuer) sau după anumite subcâmpuri din câmpul Subject. Toate aceste informații sunt conținute de fiecare certificat.



Pentru câmpul Sub Field puteți alege una din variantele de mai jos, unde O reprezintă compania care a emis certificatele (în acest caz DIGISIGN S.A.), OU reprezintă Organization Unit, CN reprezintă Common Name, E reprezintă adresa de e-mail. Toate aceste informații le găsiți pe certificate în secțiunea Details \ Subject.



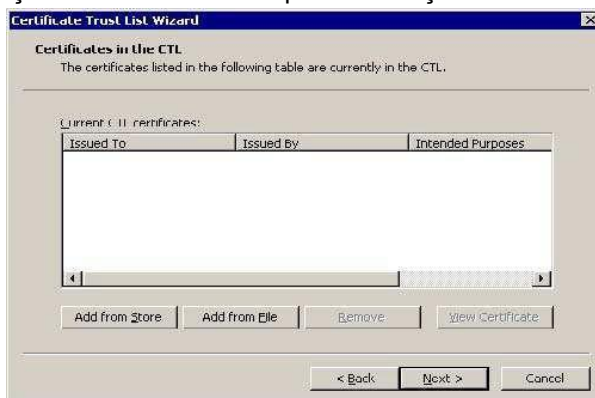

După ce ați stabilit criteriile apăsați butonul OK și veți fi solicitat să selectați una din opțiunile de mai jos. Selectați opțiunea “Accept this certificate for Logon Authentication” și selectați contul (conturile) căruia îi atribuiți această regulă. Apăsați apoi butonul Finish.



Pentru a configura opțiunea “Enable certificate trust list” apăsați butonul Edit.



Apăsați butonul Next și vi se va afișa fereastra “Certificates in the CTL”. Pentru a selecta certificatele autorității de certificare apăsați butonul Add from Store (le puteți importa direct din browser) sau Add from File (realizați importul din fișierele cu extensia.cer pe care le-ați descărcat de pe site).



Apăsați apoi butonul Next. Selectați certificatul autorității de certificare (în acest caz VERISIGN TRUSTED NETWORK) și apoi apăsați butonul OK.



Dați un nume sugestiv acestei opțiuni și apăsați butonul Next. Pentru a încheia acest proces, apăsați butonul Finish.

