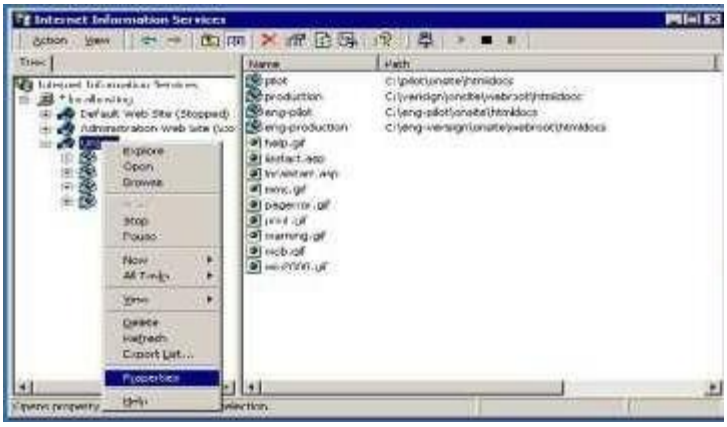
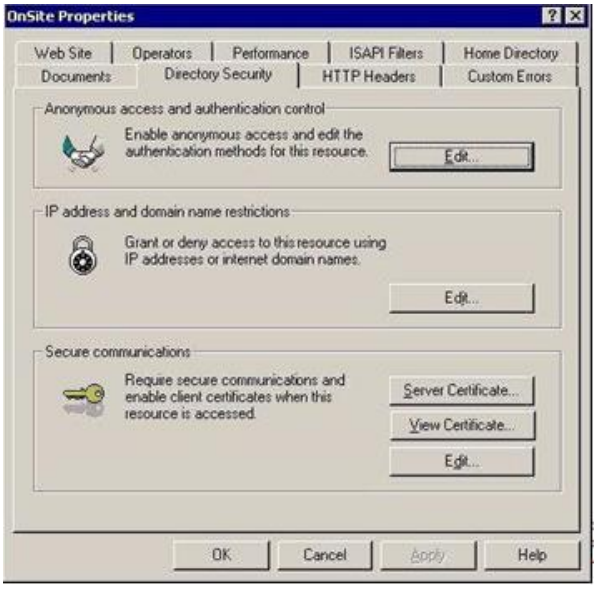
Configurarea opţiunilor pentru autentificarea pe server utilizând certificatele digitale (IIS)

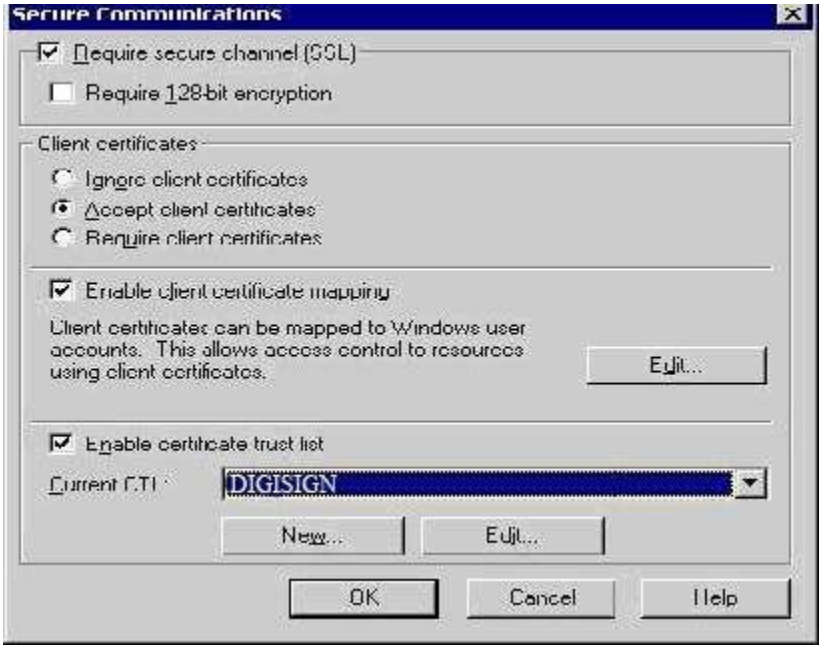
1. Selectați meniul Start ⇨ Programs ⇨ Administrative Tools ⇨ Internet Information Server. Selectați site-ul web pe care aveți instalat un certificat de server și pentru care doriți să realizați autentificarea cu ajutorul certificatelor digitale. Selectați opțiunea Properties prin *click-dreapta*.



2. Alegeți tab-ul **Directory Security** şi din secțiunea **Secure communications** apăsaţi butonul **Edit**.

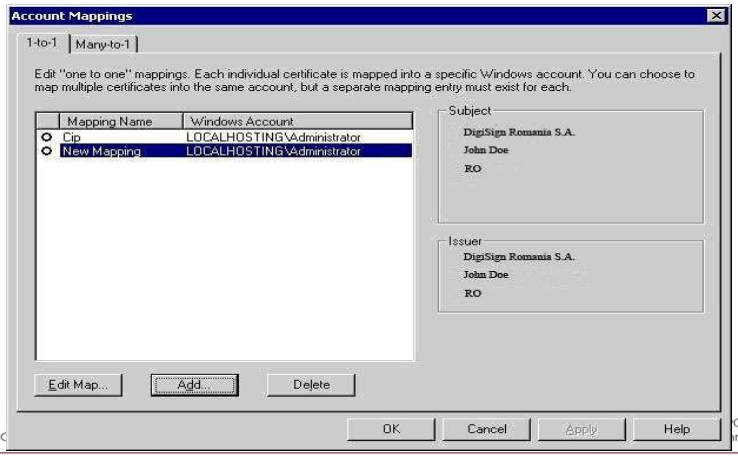


3. Bifaţi căsuţele “**Require secure channel (SSL)**”, “**Enable client certificate mapping**” şi “**Enable certificate trust list**”.



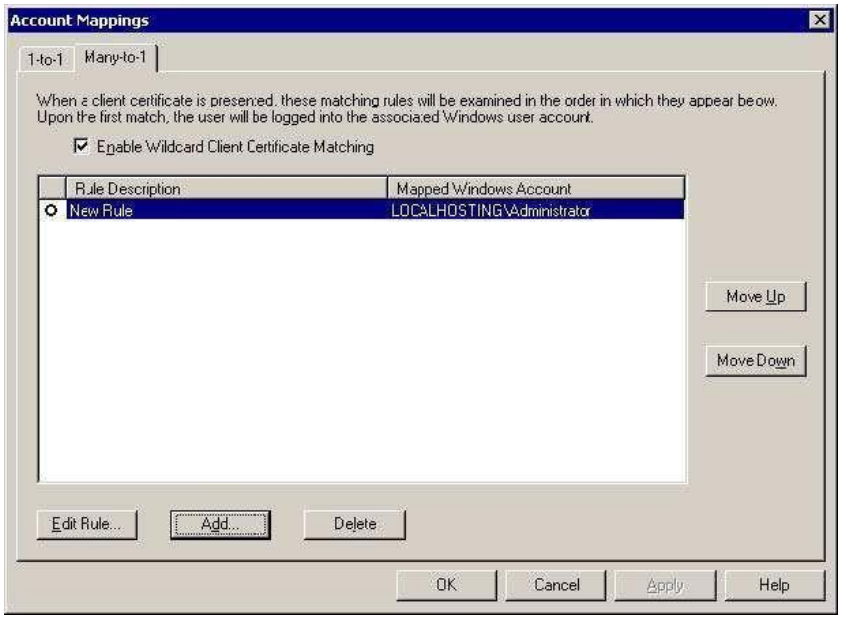
În secţiunea **Client certificates** puteţi opta pentru una din variante. În cazul în care alegeţi varianta “Accept client certificates”, autentificarea se poate realiza atât pe bază de certificate digitale cât şi pe bază de user şi parolă. Dacă optaţi pentru “Require client certificates”, autentificarea se realizează numai pe bază de certificate digitale.

În secţiunea “Enable client certificate mapping” apăsaţi butonul Edit. În această etapă puteţi opta pentru una din opţiunile 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).

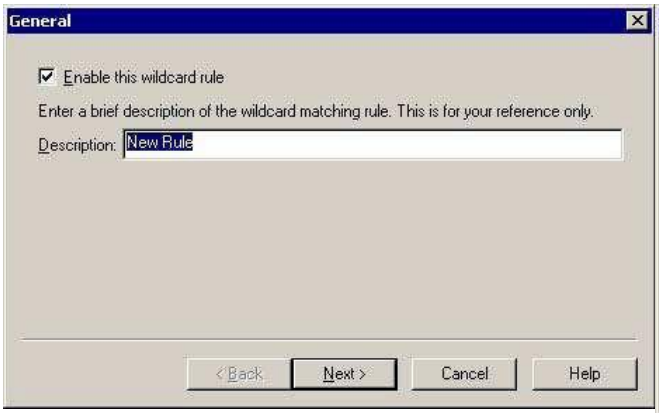


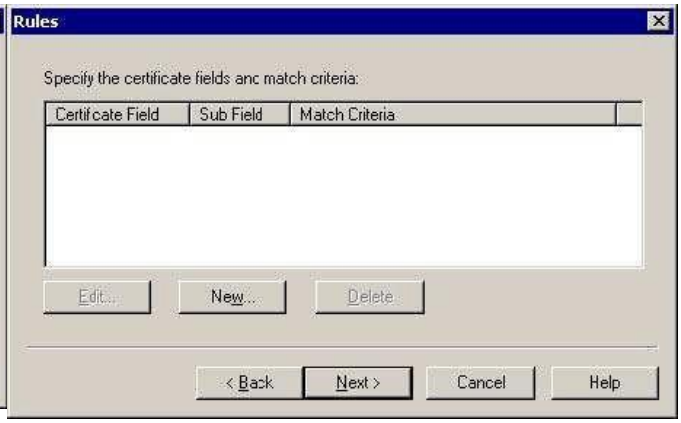
În cazul în care aţi ales opţiunea “1-to-1”, apăsaţi butonul **Add**, introduceţi numele userului (contului respectiv) şi ataşaţi-i un certificat digital valid. Certificatul respectiv se găseşte sub forma unui fişier cu extensia .cer şi conţine cheia publică.

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



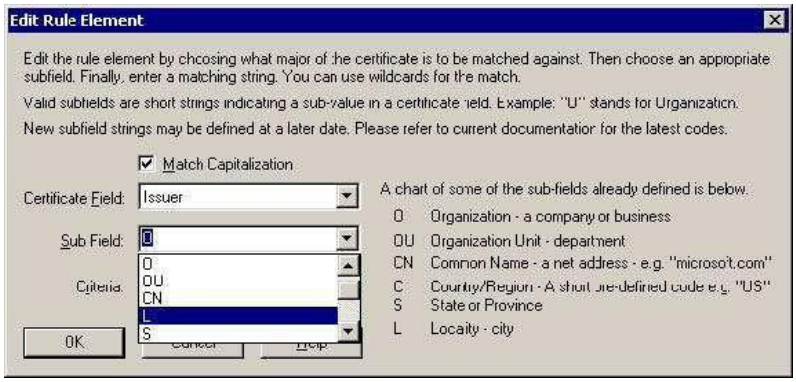
Alegeţi un nume sugestiv pentru această regulă şi apăsaţi apoi butonul **Next**. În fereastra **Rules**, apăsaţi butonul **New** pentru a crea o nouă regulă de mapare.





Veţi ajunge într-o fereastră "Edit Rule Element" unde vă puteţi alege criteriile după care doriţi să realizaţi autentificarea cu ajutorul certificatelor. Autentificarea se poate realiza după emitent (Issuer) sau după anumite subcâmpuri din câmpul Subject. Toate aceste informaţii sunt conţinute de fiecare certificat.

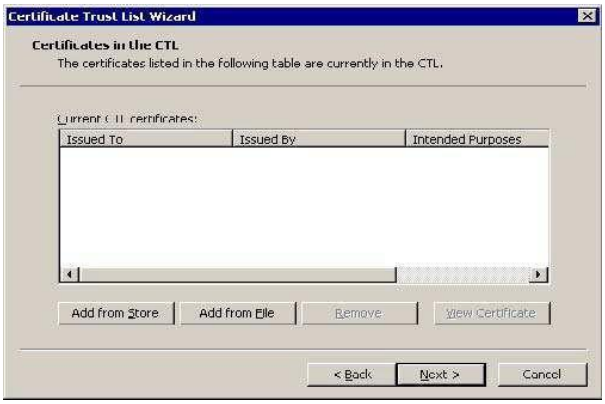
Pentru câmpul Sub Field puteţi alege una din variantele de mai jos, unde O reprezinta compania care a emis certificatele (în acest caz DIGISIGN S.A.), OU reprezintă Organization Unit, CN reprezintă Common Name, E reprezintă adresa de e- mail. Toate aceste informaţii le găsiţi pe certificate în secţiunea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



După ce aţi stabilit criteriile apăsaţi butonul OK şi veţi fi solicitat să selectaţi una din opţiunile de mai jos. Selectaţi opţiunea “Accept this certificate for Logon Authentication” şi selectaţi contul (conturile) căruia ii atribuiţi această regulă. Apăsaţi apoi butonul Finish.

Pentru a configura opţiunea “Enable certificate trust list” apăsaţi butonul Edit.

Apăsaţi butonul Next şi vi se va afişa fereastra “Certificates in the CTL”. Pentru a selecta certificatele autorităţii de certificare apăsaţi butonul Add from Store (le puteţi importa direct din browser) sau Add from File (realizaţi importul din fişierele cu extensia.cer pe care le-aţi descărcat de pe site).



Apăsaţi apoi butonul Next. Selectaţi certificatul autorităţii de certificare (în acest caz VERISIGN TRUSTED NETWORK) şi apoi apăsaţi butonul OK.

Daţi un nume sugestiv acestei opţiuni şi apăsaţi butonul Next. Pentru a încheia acest proces, apăsaţi butonul Finish.