

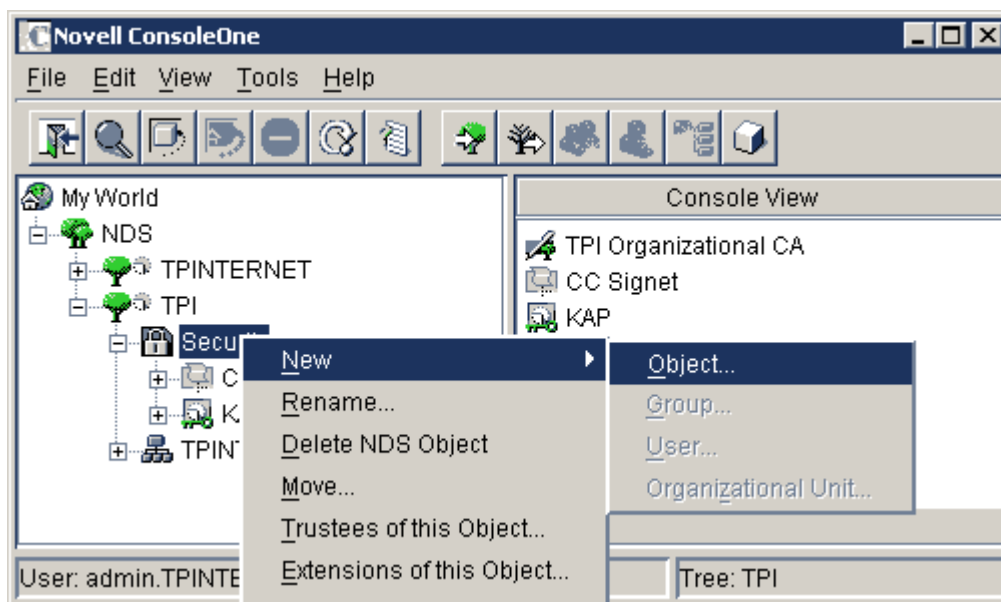
# Procedura pozyskania i instalacji certyfikatów SSL dla **Novell Netware LDAP Server 3.x**

## 1. Generowanie pary kluczy oraz wniosku o certyfikat CSR.

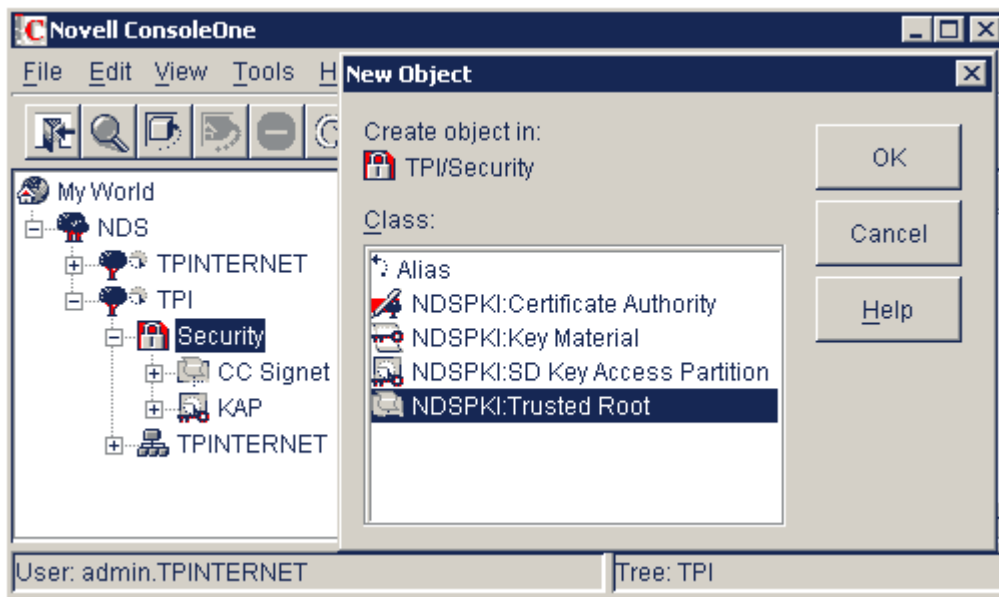
W celu wygenerowania pary kluczy oraz żądania certyfikatu (CSR) należy skorzystać z konsoli administracyjnej ConsoleOne w wersji min. 1.2b. Na serwerze powinno być zainstalowane oprogramowanie Novell Certificate Server. Pierwszym etapem będzie stworzenie bazy przechowującej certyfikaty Trusted Root w NDS. Będzie to obiekt kontenera Trusted Root w kontenerze Security.

**Uwaga!** Aby móc stworzyć obiekt kontenera Trusted Root powinniśmy posiadać uprawnienia Create do kontenera Security.

Po uruchomieniu programu ConsoleOne należy rozwinąć nasze Drzewo i zaznaczyć obiekt kontenera Security. Prawym przyciskiem myszki wybieramy z menu New (nowy) oraz Object (obiekt)



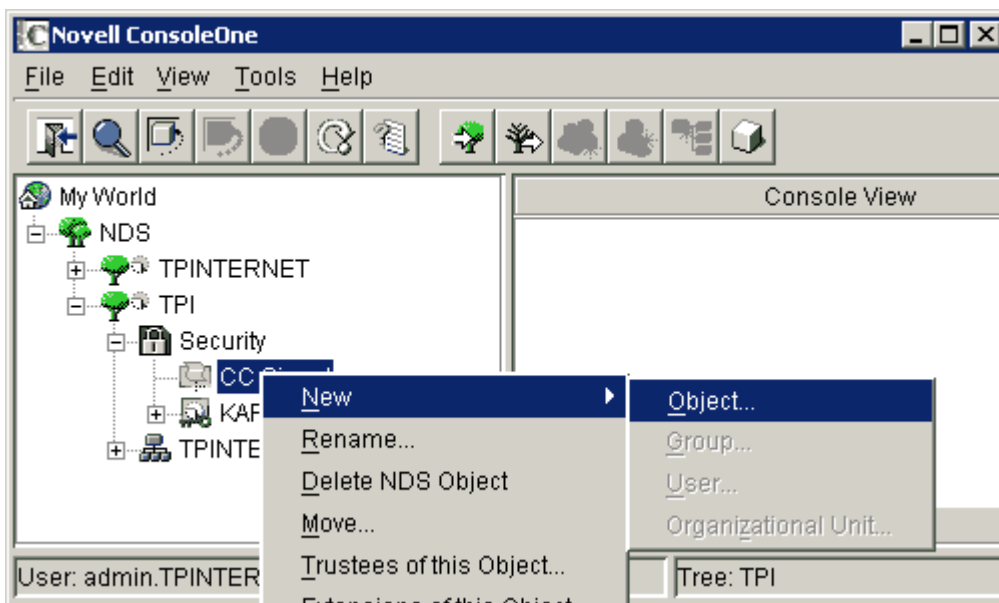
i wybieramy obiekt **NDSPKI:Trusted Root Container** i wybór potwierdzamy klawiszem **OK**.



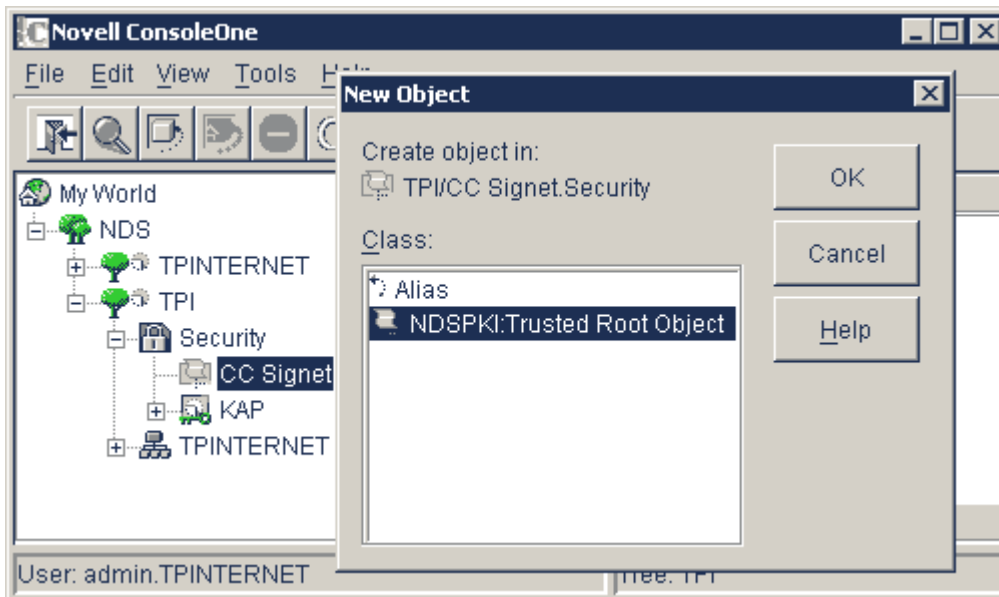
Następnie system zapyta nas o nazwę tego kontenera i podajemy dowolną nazwę np. CC Signet. Kolejnym krokiem będzie utworzenie w kontenerze o nazwie CC Signet obiektów Trusted Root, które będą przechowywały certyfikaty Głównego Urzędu CA oraz Urzędu CA Klasy 1.

**Uwaga!** Aby móc stworzyć obiekt Trusted Root w kontenerze CC Signet powinniśmy posiadać uprawnienia Create do kontenera CC Signet.

W celu utworzenia obiektu **Trusted Root** należy podświetlić utworzony kontener CC Signet i po wciśnięciu prawego przycisku myszy wybrać **New** (nowy) oraz **Object** (obiekt)



i wybieramy obiekt NDSPKI: **Trusted Root Object** i wybór potwierdzamy klawiszem **OK**.

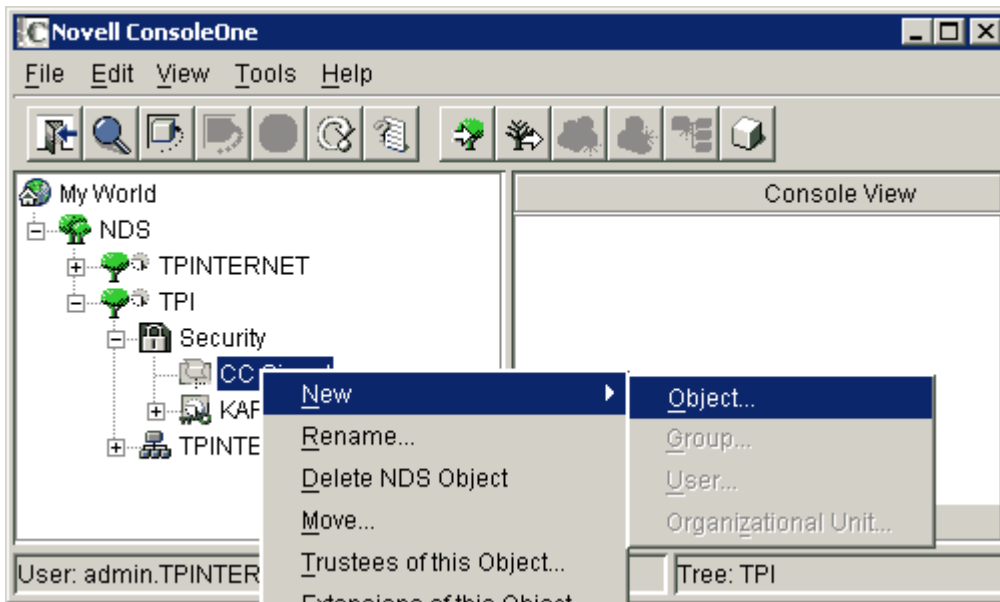


Następnie system zapyta nas o nazwę dla tego obiektu i podajemy dowolną nazwę np. CC Signet Root CA. W tym samym oknie musimy wkleić źródło certyfikatu Głównego Urzędu CC Signet - Root CA poprzez bezpośrednie wklejenie go ze schowka (paste) lub wczytanie go z pliku. Po wklejeniu źródła wybieramy **Finish**.

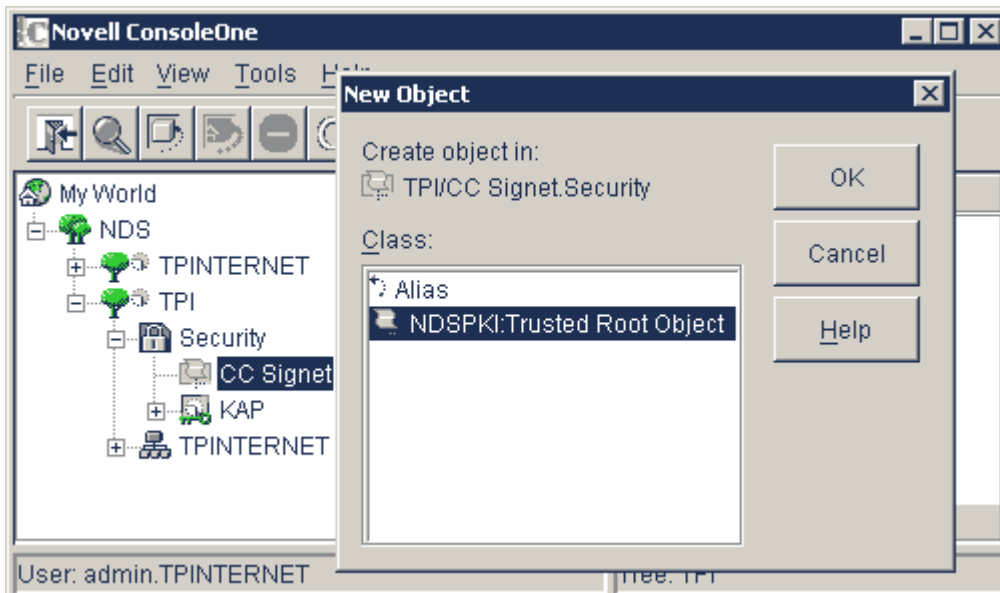


Teraz analogicznie tworzymy drugi obiekt Trusted Root w kontenerze CC Signet przechowujący certyfikat Urzędu CA Klasy 1.

W celu utworzenia obiektu Trusted Root należy podświetlić utworzony kontener CC Signet i po wciśnięciu prawego przycisku myszy wybrać **New** (nowy) oraz **Object** (obiekt)



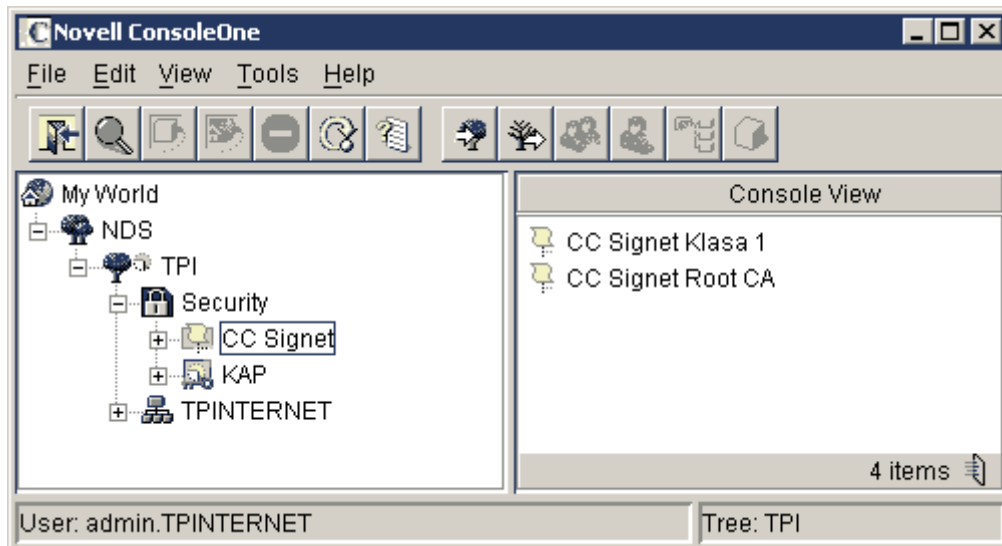
i ponownie wybieramy obiekt NDSPKI: **Trusted Root Object** i wybór potwierdzamy klawiszem **OK**.



Następnie system zapyta nas o nazwę dla tego obiektu i podajemy dowolną nazwę np. CC Signet Klasa 1. W tym samym oknie musimy wkleić źródło certyfikatu Urzędu poprzez bezpośrednie wklejenie go ze schowka (paste) lub wczytać go z pliku i potwierdzić klawiszem **Finish**.

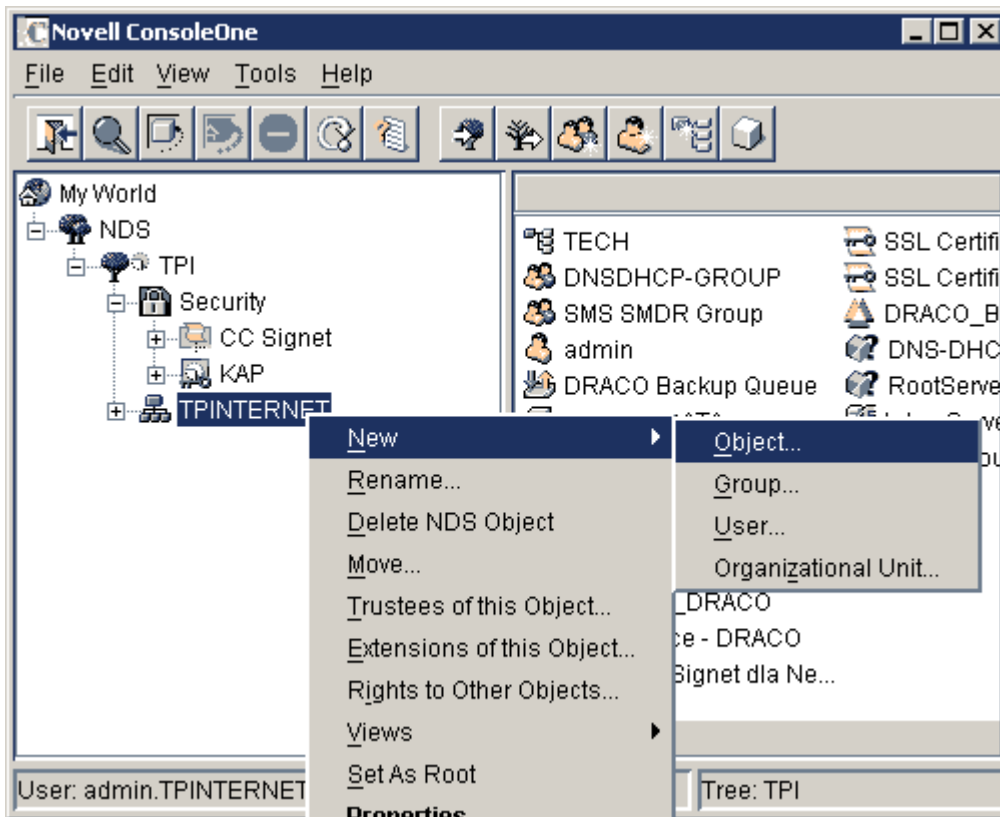


W kontenerze CC Signet powinniśmy mieć dwa obiekty o nazwach: **CC Signet Root CA** oraz **CC Signet Klasa 1**, które przechowują certyfikaty ww. urządzeń.

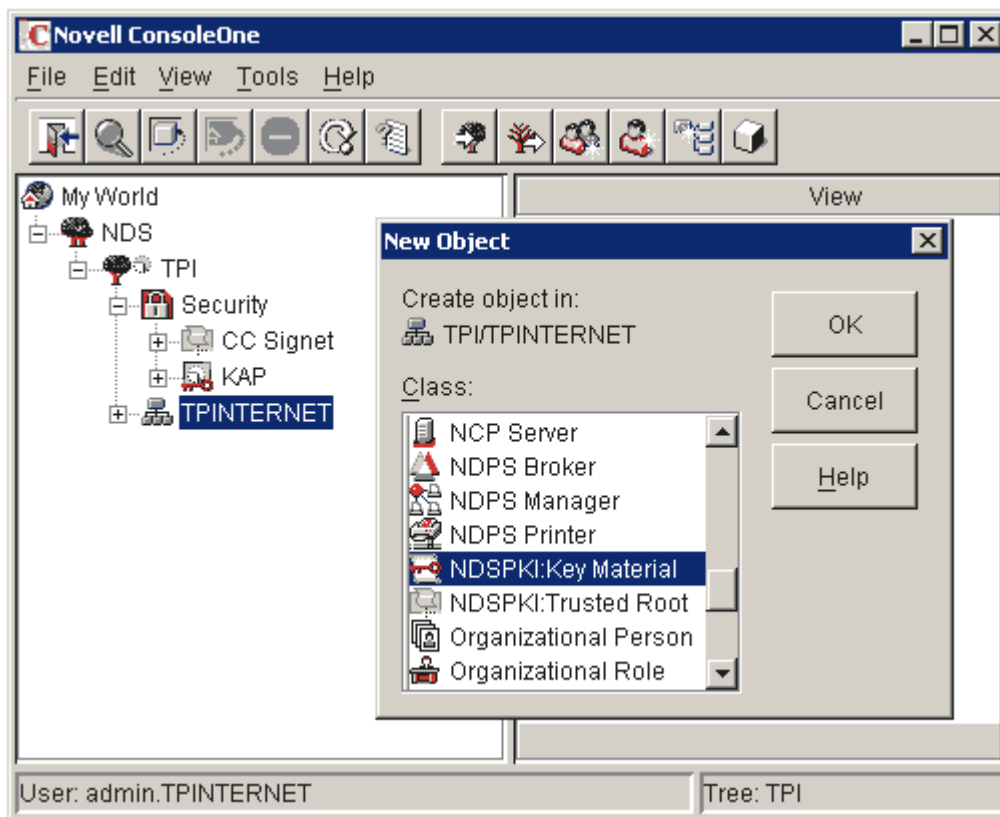


W tym momencie możemy przejść do wygenerowania pary kluczy oraz żądania o certyfikat (CSR) dla naszego serwera LDAP. Tworzymy obiekt **Key Material** w kontenerze serwera, w którym znajduje się obiekt **LDAP Server** (w naszym przypadku będzie to kontener TPINTERNET).

W tym celu należy podświetlić kontener **TPINTERNET** i klikając prawym przyciskiem myszy wybrać **New** (nowy) oraz **Object** (obiekt)



i wybieramy obiekt NDSPKI: **Key Material** i wybór potwierdzamy klawiszem **OK**.



Następnie system zapyta nas nazwę serwera (dla którego wystawić certyfikat). Jeżeli w kontenerze znajduje się jeden serwer należy wybrać właściwy (ten na którym uruchomiony jest serwer LDAP). W naszym przypadku będzie to serwer DRACO. Następnie system prosi o podanie nazwy obiektu.

Wpisujemy dowolną nazwę, np. **Certyfikat CC Signet dla Netware**. Ostatnim polem wyboru w tym menu jest wybór metody tworzenia certyfikatu i wybieramy opcję **Custom** i kontynuujemy tworzenie certyfikatu przez naciśnięcie **Next**.

**Create Server Certificate (Key Material)**

Specify the server which will own the certificate.  
Specify the certificate name and creation method.

Server: DRACO

Certificate name: Certyfikat CC Signet dla Netware

Creation method

Standard  
The standard method uses the default parameters.

Custom  
The custom method allows you to specify the parameters.

< Back Next > Cancel Finish Help

W kolejnym menu system pyta o centrum autoryzacji podpisujące nasz certyfikat. Wybieramy opcję **External certificate authority** (zewnętrzny urząd certyfikacyjny) i klikamy na **Next**.

**Create Server Certificate (Key Material)**

Specify the certificate authority which will sign this certificate.

Organizational certificate authority

Other NDS certificate authority  
DRACO.TPINTERNET

External certificate authority

< Back Next > Cancel Finish Help

W kolejnym oknie system pyta o długość klucza. W zależności od potrzeb decydujemy się na klucz o odpowiedniej długości. W naszym przykładzie zdecydujemy się na klucz o długości 1024 bitów i klikamy ponownie na **Next**.

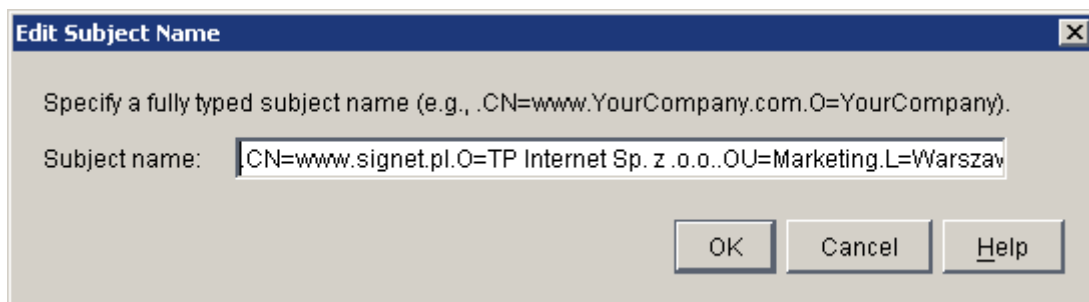


W kolejnym oknie musimy wybrać parametry certyfikatu takie jak **Subject Name** i wybór algorytmu podpisywania. W polu **Signature Algorithm** zostawiamy algorytm **RSA encryption with SHA-1 hash**. Należy zmienić pole **Subject Name** wybierając opcję **Edit**. W polu dialogowym wpisując parametry nie używamy polskich znaków oraz znaków specjalnych. W naszym przykładzie stworzymy certyfikat dla serwera zlokalizowanego w Warszawie w organizacji TP Internet Sp. z o.o. w dziale Marketing o pełnej nazwie DNS'owej www.signet.pl. Poszczególne parametry zaczynamy od kropki, np.

.CN=www.signet.pl.O=TP Internet Sp. z .o.o..OU=Marketing.L=Warszawa.ST=Mazowieckie.C=PL

**Uwaga!** W polu CN musi znajdować się pełna nazwa DNS (fqdn) naszego serwera LDAP np. [www.signet.pl](http://www.signet.pl)

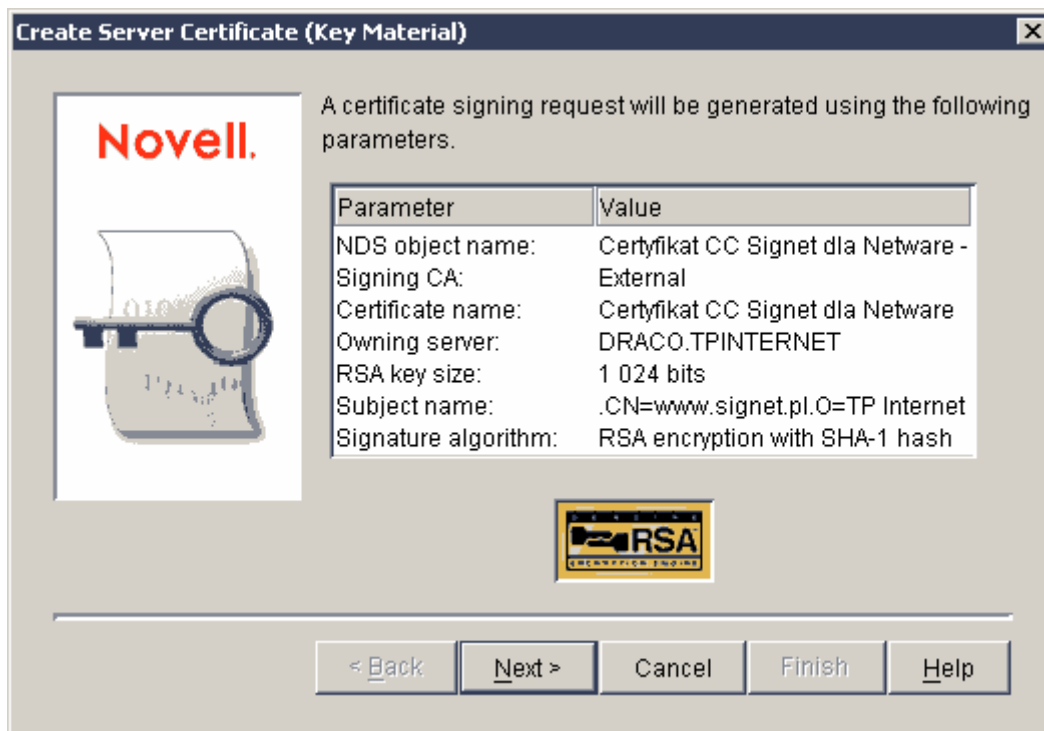
Po wpisaniu tych parametrów potwierdzamy wybór klawiszem **OK**.



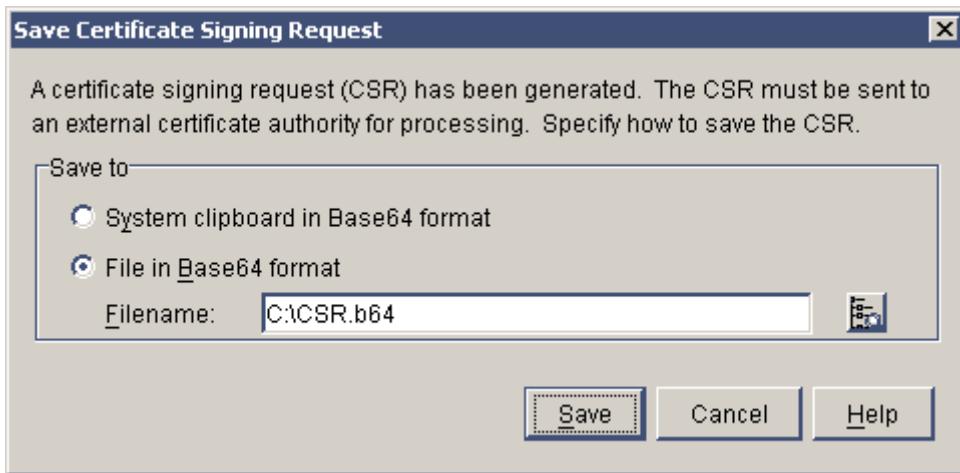
i kontynuujemy klikając **Next**.



Pojawi się okno wyświetlające wszystkie opcje naszego żądania o certyfikat (CSR).



Klikając **Finish** program przystąpi do generowania pary kluczy oraz żądania certyfikatu (CSR). Czas potrzebny do wykonania tego zadania zależy od długości klucza, obciążenia serwera oraz jego mocy obliczeniowej. Po wygenerowaniu pary kluczy oraz żądania certyfikatu (CSR) mamy możliwość zapisania źródła żądania certyfikatu (CSR) do schowka systemowego (System clipboard in Base64 format) lub bezpośrednio do pliku (File in Base64 format).



Przykładowy plik wniosku (CSR) powinien wyglądać mniej więcej tak:

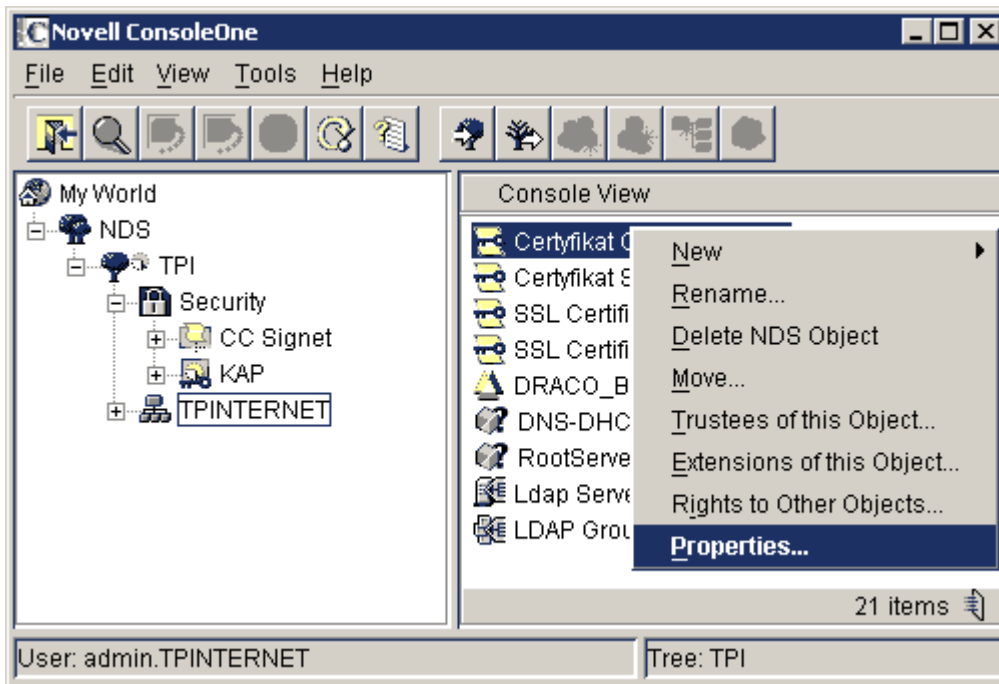
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICyzCCAbMCAQAwgYUxFjAUBgNVBAMTDXd3dy5zaWduZXQucGwxIDAeBgNVBAoT
F1RQIEludGVybWV0IFNwLiB6IC5vLm8uMRIwEAYDVQQLEw1NYXJrZXRpbmcxETAP
BgNVBACTFdhenN6YXdhMRUwEwYDVQQIEw1NYXpvd211Y2tpZSAxZzAJBgNVBAYT
AlBMMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzf9zlxQCnA7dPor
XjIjhSKfFGE/7WOUb/+eEAGqsuiXfUbMtU+csdQwlsU5MB7Ty7yf+k2RYq04q7Pg
9YhZIEFIrDQdA4UXU026dSYfk+eCbIPVvxn6pMfVjGhvUMoP8ppsFfLdgMqQ+i7
5g4ZiJ/GNeh70/91qNCuZBobozh/filFozSKo8VG2HOxLALA98sLOTMpa8gERfmB
Smh7xCq71Iw3hXq439oZ3jq6W9W10oC7bJ8Kwv1lHIVa1TC1RLd+X+/rx9wM52YO
fEKskKUXMMBQKLxLhVCpeh9VhnLhOjd/laGvg4BIQai6YgHdErSFQZP8ed+SQz3l
9xzsGwIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBADDW1lBAXAysFW8K6agqPyA
z9Gsc7UGyzBqicxevp+GCFJB6ADYtcO3qgr25/p3tnekgP2xc650QgriBKjPH2Ed
HVCeRFaFBIOTJJVnUv9PcEwYsQmj2eWniyWmrq9TP9nIpvJqit7YhmoP3mOicdUm
1GQBcKZKKsx2355xJtSZAcMy+jSEdbiTAOxKfqv4qcaa6rL4yjd8xsSz0Ym9BCOs
Ud+Yz0UHnNZbQreNK5hzukSNv8bv6kI8S6eBXkM7lDejguRl5jR+cqo2NKxDf3hN
GqZBY3luqa34PhL6celjDfFJRWf9LzD12UcOBaGGY46SmUu4BfT+ncgCmbqD
pD4=
-----END NEW CERTIFICATE REQUEST-----
```

Tak wygenerowany wniosek wklejamy na stronie Centrum Certyfikacji Signet.

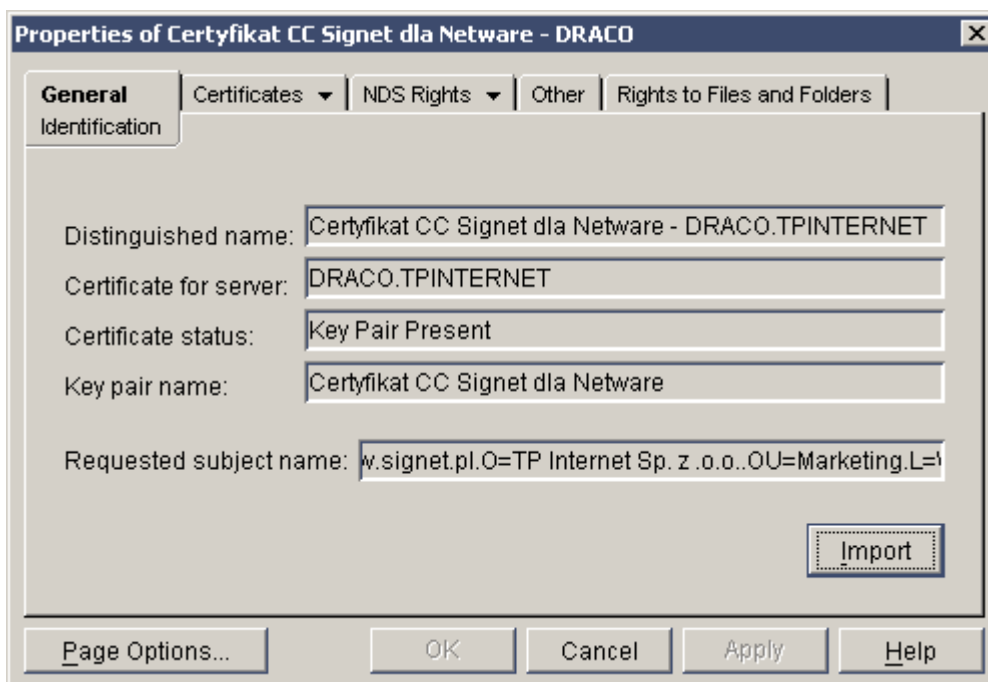
## 2. Instalacja certyfikatu na serwerze Netware LDAP Server

Po wysłaniu żądania certyfikatu do Centrum Certyfikacji Signet i otrzymaniu certyfikatu możemy przystąpić do jego instalacji.

W tym przypadku podświetlamy utworzony obiekt **Certyfikat CC Signet dla Netware** (Key Material) i klikając prawym przyciskiem myszy wybieramy z menu opcję **Properties**.



Pojawi się okno z właściwościami obiektu **Certyfikat CC Signet dla Netware**, w którym pierwsza zakładka General-Identification przedstawia m.in. status certyfikatu: **Key Pair Present**.



Po wybraniu opcji **Import** wklejamy certyfikat Urzędu CA Klasy 1, który możemy wyeksportować z obiektu CC Signet Klasa 1 lub ściągnąć ze strony [www.signet.pl](http://www.signet.pl)



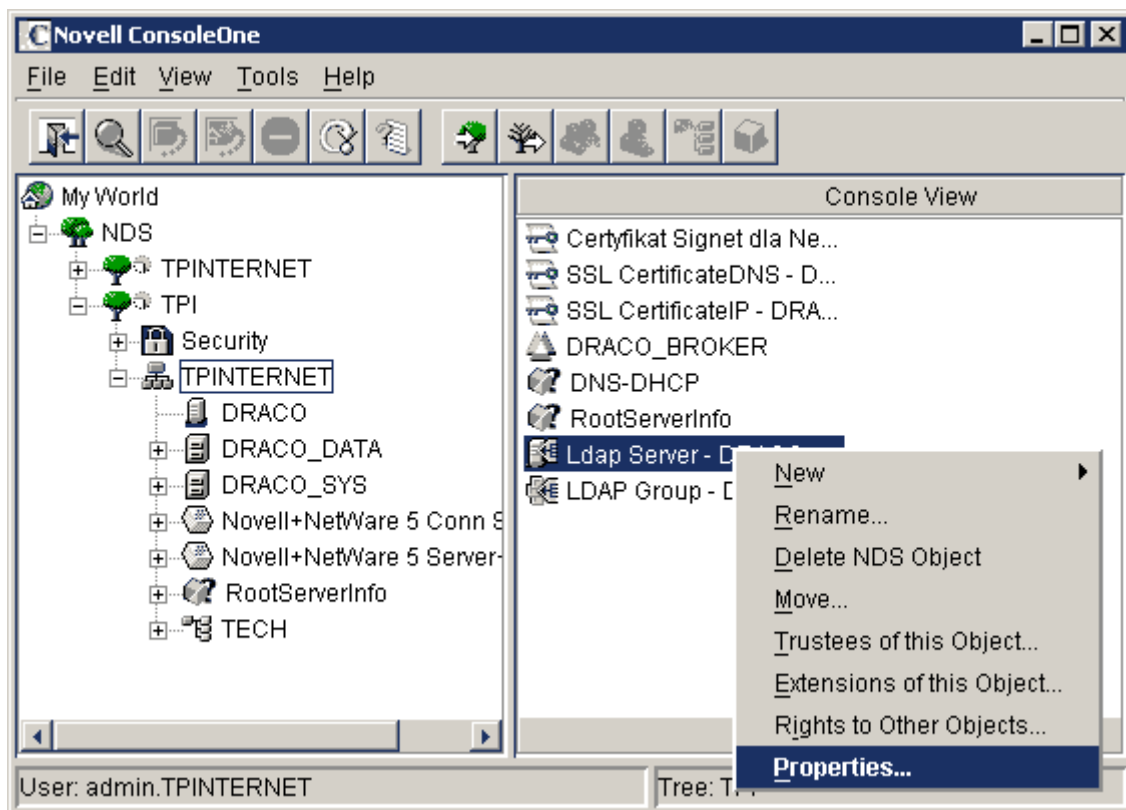
i wybieramy opcję **Next**. W następnym oknie wklejamy certyfikat dla naszego serwera otrzymany z CC Signet i klikamy przycisk **Finish**.



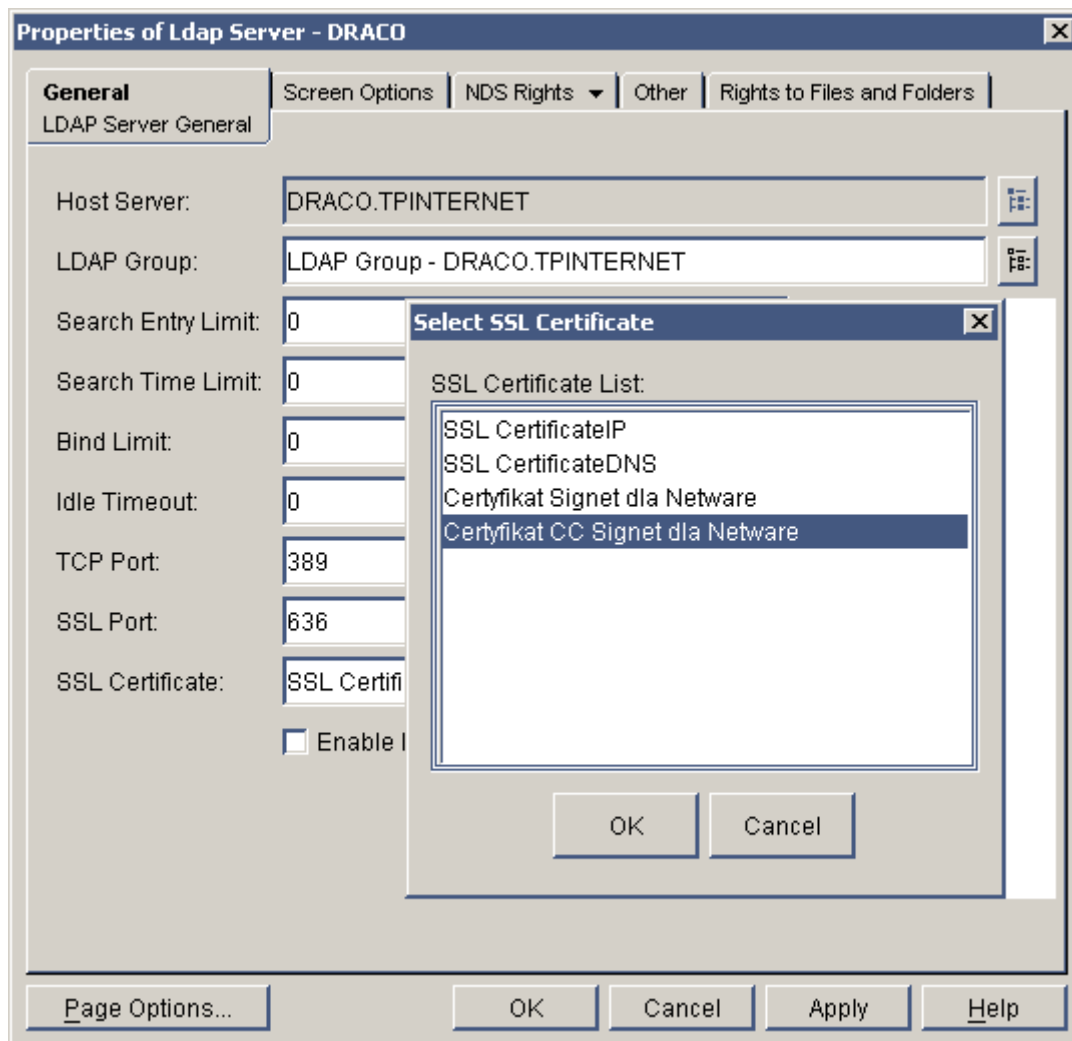
Jeżeli wszystkie powyższe czynności wykonaliśmy prawidłowo, pole Certificate Status obiektu "Certyfikat CC Signet dla Netware" powinno zmienić status z Key Pair Present na Certificate Present. Możemy to sprawdzić klikając na właściwości (properties) obiektu "Certyfikat CC Signet dla Netware" w oknie informacyjnym w zakładce General-Identification pole Certificate Status. Szczegółowe informacje o certyfikatach wystawcy (CC Signet) i podmiotu (nasz serwer) znajdziemy w drugiej zakładce Certificates.

Pozostaje teraz skojarzyć gotowy certyfikat z naszym serwerem LDAP.

Korzystając z **ConsoleOne** prawym przyciskiem myszy podświetlamy obiekt **LDAP Server** i z menu wybieramy **Properties** (Właściwości).



Pojawi się okno z właściwościami obiektu serwera LDAP. W polu **SSL Certificate** podmieniamy standardowy certyfikat na **Certyfikat CC Signet dla Netware**. Należy zwrócić uwagę, żeby opcja **Disable SSL Port** nie była zaznaczona. Po wybraniu naszego certyfikatu potwierdzamy wybór klawiszem **OK**.



Kliknięcie na przycisk **Apply** spowoduje uruchomienie serwera LDAP z nową konfiguracją.