

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

LOTUS DOMINO 7

Użycie certyfikatów niekwalifikowanych w oprogramowaniu
LOTUS DOMINO 7 – serwer WWW / pocztowy

wersja 1.1

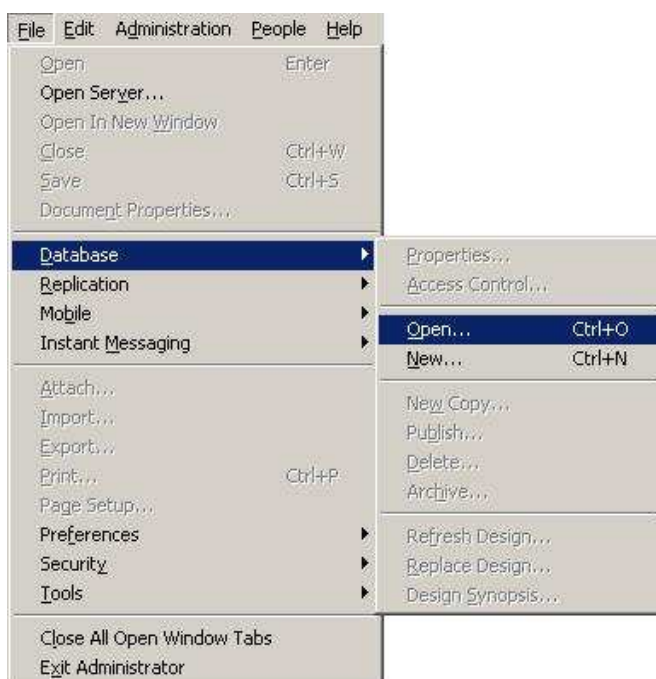
Spis treści

| | |
|--|-----------|
| 1. TWORZENIE CERTYFIKATU DLA ADRESU JEDNOZNACZNEGO | 3 |
| 1.1. TWORZENIE PLIKU KEY RING | 3 |
| 1.2. TWORZENIE ŻĄDANIA CERTYFIKATU (CSR) | 7 |
| 1.3. TWORZENIE CERTYFIKATU NA PODSTAWIE WYGENEROWANEGO ŻĄDANIA (CSR) | 9 |
| 1.4. POBIERANIE CERTYFIKATU CERTUM CA I CERTYFIKATÓW POŚREDNICH | 10 |
| 1.5. INSTALOWANIE CERTYFIKATU CERTUM CA I CERTYFIKATÓW POŚREDNICH | 11 |
| 1.6. POBIERANIE I INSTALOWANIE CERTYFIKATU SERWERA | 14 |
| 2. TWORZENIE CERTYFIKATU DLA ADRESÓW WIELOZNACZNYCH | 17 |
| 3. KONFIGUROWANIE SERWERA DO POŁĄCZEŃ HTTPS | 17 |
| 4. KONFIGUROWANIE SERWERA DO OBSŁUGI WITRYN WIRTUALNYCH | 19 |

1. Tworzenie certyfikatu dla adresu jednoznacznego

1.1. Tworzenie pliku Key Ring

Uruchamiamy program *Domino Admin* i otwieramy bazę *certsrv.nsf*. Dokonamy tego przez użycie kombinacji klawiszy *CTRL + o* (i wskazanie odpowiedniej bazy) lub wchodząc w menu: *file -> Database -> Open...* :



Z okienka *Server* wskazujemy serwer, dla którego generujemy klucze:



i otwieramy bazę *certsrv.nsf* (*Server Certificate Admin*):



W otwartym *Menu* w lewym panelu wybieramy *Create Key Rings & Certificate*, po czym w głównym oknie wchodzimy w *Create Key Ring* (co rozpocznie proces certyfikacji):



W polu *Key Ring Information* wprowadzamy nazwę pliku klucza *Key Ring* (domyślnie *keyfile.kyr*) oraz hasło, które zabezpieczy tenże plik z kluczami (musi być odpowiednio silne!!!):

| Key Ring Information | Quick Help |
|---------------------------------|---|
| Key Ring File Name: keyfile.kyr | Specify the name and password for the key ring file. Note: You'll be referring to the key ring information you enter here in subsequent steps as you create and install certificates into the key ring. |
| Key Ring Password: ***** | |
| Confirm Password: ***** | |

Zmieniamy wielkość klucza z 512 do zalecanej 1024-bitowej długości:

| Key Size | Select Keywords |
|----------------|--------------------------|
| Key Size: 1024 | Keywords: 512 1024 |

Uzupełniamy pola z informacjami o naszym certyfikacie.

Country (C) - dwuliterowy symbol kraju (PL). Należy użyć kodu ISO, np. poprawnym kodem Polski jest PL (duże litery), a nie pl czy RP.

State / Province (ST) - nazwa województwa, np.: Zachodniopomorskie. Nie należy stosować skrótów.

City or Locality (L) - nazwa miasta lub wsi, np.: Szczecin, Kozia Wolka, Warszawa.

Organization Name (O) - pełna nazwa swojej organizacji / firmy, np.: Moja Firma

Organizational Unit (OU) - jeżeli zachodzi taka potrzeba, można wypełnić to pole, wstawiając nazwę działu np. Oddział w Moja Firma

Common Name (CN) - **bardzo ważne pole!** Musi się tutaj znaleźć pełna nazwa DNS (fqdn) serwera np.: www.mojserwer.pl, mojadomena.plm *.mojserwer.pl.

UWAGA: Używanie znaków specjalnych % ^ \$ _ lub polskich znaków diakrytycznych: Żółć przy podawaniu tych informacji spowoduje nieprawidłowe wygenerowanie certyfikatu !!!

| Distinguished Name | |
|----------------------|--|
| Common Name: | <input type="text" value="mojserwer.pl"/> |
| Organization: | <input type="text" value="Moja Firma"/> |
| Organizational Unit: | <input type="text" value="Oddzial w Moja Firma (optional)"/> |
| City or Locality: | <input type="text" value="Szczecin (optional)"/> |
| State or Province: | <input type="text" value="Zachodniopomorskie (no abbreviations)"/> |
| Country: | <input type="text" value="PL (two character country code)"/> |

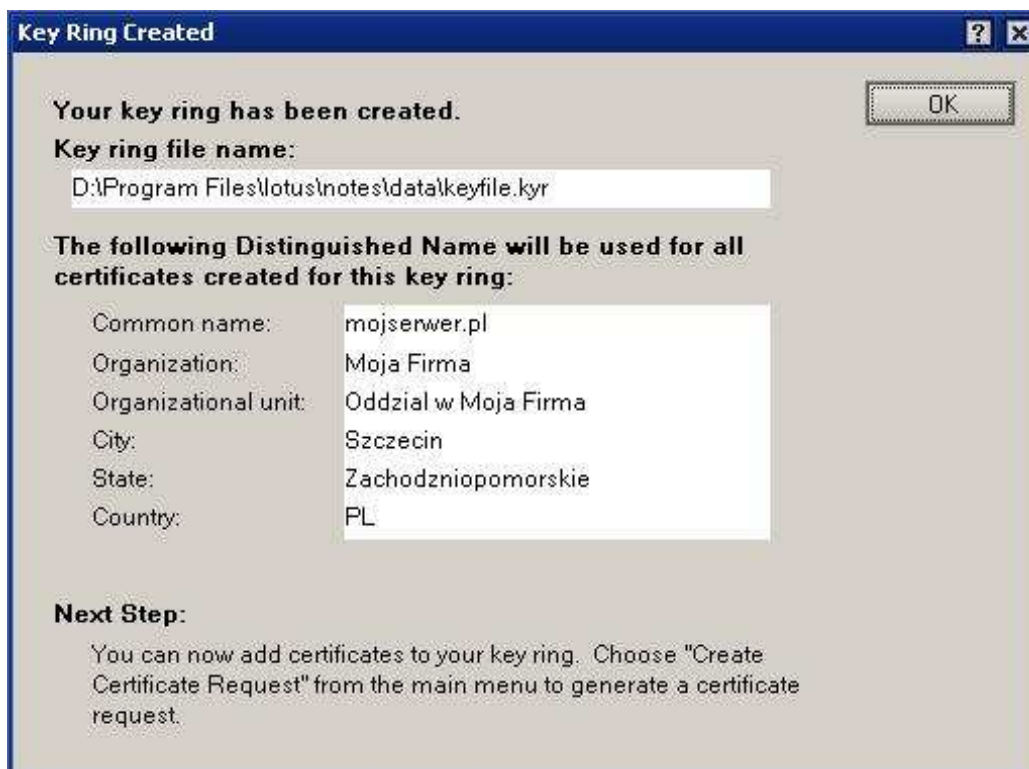
The Distinguished Name is the information about your site that will appear in any certificates you create.

Note: Make sure the Common Name matches the URL of your site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.

Po podaniu tych informacji klikamy *Create Key Ring*:

Create Key Ring

Kreator poinformuje nas o pomyślnym wygenerowaniu *Key Ring*:



1.2. Tworzenie żądania certyfikatu (CSR)

Aby utworzyć żądanie certyfikatu, z głównego Menu wybieramy *Create Certificate Request*:

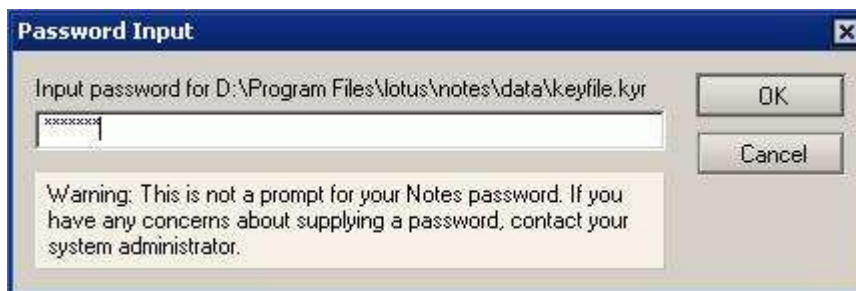


Wskazujemy plik z kluczem *Key Ring* oraz metodę wysłania żądania do CERTUM (wkleimy ją ręcznie) oraz klikamy *Create Certificate Request*:

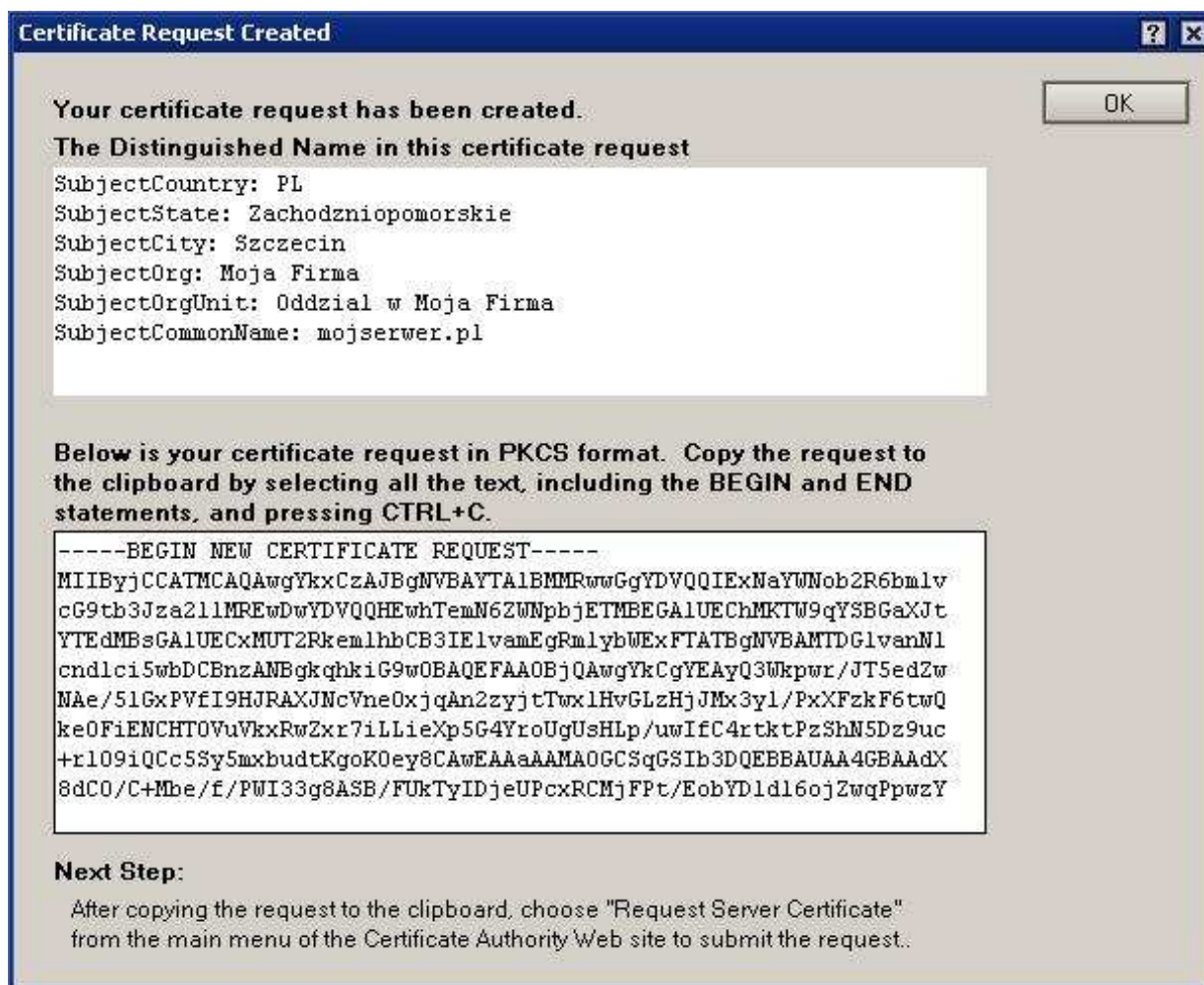
| Key Ring Information | |
|----------------------|---|
| Key Ring File Name | D:\Program Files\lotus\notes\data\keyfile.kyr |

| Certificate Request Information | |
|---------------------------------|---|
| Log Certificate Request | Yes |
| Method | <input checked="" type="radio"/> Paste into form on CA's site <input type="radio"/> Send to CA by e-mail |

Wpisujemy hasło zabezpieczające klucz prywatny:



Ujrzymy nasze żądanie w formacie PKCS - zapiszmy je na dysku. CSR powinno mieć postać podobną do poniższej.



UWAGA: W celu wklejania certyfikatu do pliku należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--", używając do tego celu edytora tekstowego np. Notepad i myszki. **Nie należy używać do tej operacji Worda, czy innego procesora tekstowego!**

1.3. Tworzenie certyfikatu na podstawie wygenerowanego żądania (CSR)

Mając wygenerowane żądanie wypełniamy formularz zgłoszeniowy i wklejamy CSR na stronie CERTUM (www.certum.pl) -> *Oferta* -> *Certyfikaty niekwalifikowane* -> *Zabezpieczanie serwerów* -> *Serwery WWW* -> wybieramy, który certyfikat chcemy kupić i na dole strony wybieramy *Kup certyfikat*).

Pobierz certyfikat Private WEB Server (niekwalifikowany)

Żądanie certyfikatu

W poniższe pole wstaw żądanie certyfikatu zgodne z PKCS#10.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgY4xCzAJBgNVBAYTAiBMMRswGQYDVQQIEsJaYWNob2RuaW9w
b21vcnNraWUxETAPBgNVBACtCFN6Y3plY2luMQ8wDQYDVQQKEwZDZXJ0dW0xZjAU
BgNVBAMTDTEwLjEwMC4xMC4xMjIwLjEwMC4xMjIwLjEwMC4xMjIwLjEwMC4xMjIw
Y3pAY2YyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYyYy
rbeOpj3N5hTqUCJY0GwQfNyq+3gSBqBQagVghY64TNKI6636Sd7GvtQWMg7ycbzV
bAzHmHci8ML4eMrBDvetbllNxiql/WTWiQmVZUoA0aJl2OzVjF3O0juLIoQLQONA
X+SyrQ5Z2Z2ka7+dA7AQ2Sn4dkbKJPgAFwIDAQABoAAwDQYJKoZIhvcNAQEEBQAD
gYEAaHg9qUvjzTQfVccsuJtBKPMr4yw4mE9976GBigAT1EAWRTu85yEqsS0SUHw
qndhGbkK4srC82sg1736GNUUgjbT9hAb2e3ehHv+ava/2VYsz6Mzx7xpFssMa2YL
SAKGGHrS1eTLaQ84hzgnf+0HNQvJ53WLUaMpYjwAa2t0KyM=
-----END CERTIFICATE REQUEST-----
```

Adres email

Podaj adres e-mail, na który zostaną wysłane dalsze instrukcje postępowania.

E-mail:

Oświadczenie

ZANIM ZŁOŻYSZ WNIOSEK O WYDANIE CERTYFIKATU, POTWIERDZISZ GO, BĄDŹ UŻYJESZ DO REALIZACJI PIERWSZEGO PODPISU POWINIENIEŚ PRZECZYTAĆ TEKST NINIEJSZEGO OŚWIADCZENIA. JEŚLI NIE ZGADZASZ SIĘ Z WARUNKAMI NINIEJSZEGO OŚWIADCZENIA, NIE SKŁADAJ WNIOSKU O WYDANIE CERTYFIKATU, NIE POTWIERDZAJ I NIE UŻYWAJ GO.

Niniejsze oświadczenie obowiązuje od momentu przestania przez Ciebie wniosku o wydanie certyfikatu do CERTUM - Powszechne Centrum Certyfikacji. Przedkładając wniosek o wydanie

Potwierdzam oświadczenie

UWAGA: W celu wklejania certyfikatu na stronie należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--" (razem z tymi liniami!!!), używając do tego celu edytora tekstowego.

Upewniamy się, że w polu *E-mail* jest wpisany poprawny adres (na ten adres zostaną wysłane dalsze instrukcje), oraz, że zaznaczyliśmy pole *Potwierdzam Oświadczenie* i klikamy *Dalej*.

Pojawi się strona, na której możemy się upewnić, że nasze żądanie CSR zostało wygenerowane na prawidłowe dane.

Uwaga: Należy się upewnić, że w polu podmiot jest wpisana poprawna nazwa naszej strony (jesli kupujemy certyfikat na domenę www.mojastrona.com upewnijmy się, że ta nazwa widnieje w tym polu!!!)

Upewniwszy się, co do poprawności wprowadzonych danych klikamy *Dalej*:

Pobierz certyfikat Private WEB Server (niekwalifikowany)

Weryfikacja danych

 Poniżej znajdują się dane, które zawarte są w żądaniu certyfikatu. Jeśli zachodzi potrzeba modyfikacji danych, należy anulować dalsze wypełnianie formularza i przygotować nowe żądanie PKCS#10

Kraj: PL
Województwo: Zachodniopomorskie
Miasto: Szczecin
Firma: Certum
Podmiot: **10.100.10.122**
E-mail: mproszkiewicz@certum.pl

Jeżeli powyższe dane są poprawne, naciśnij "Dalej", aby kontynuować proces wydawania certyfikatu.

Dalej

Pojawi się okno z informacją o wymaganych dokumentach niezbędnych do zakończenia procesu uzyskania certyfikatu.

1.4. Pobieranie certyfikatu Certum CA i certyfikatów pośrednich

Aby pobrać certyfikat Certum CA lub certyfikaty pośrednie należy wejść na stronę www.certum.pl do działu *Obsługa certyfikatów* → *Zaświadczenia i klucze*. Po wybraniu certyfikatu należy wybrać opcję *Certyfikat dla serwerów WWW*.

| Główny klucz urzędu - Certum CA | |
|---|---|
| Nr seryjny: | 10020 |
| Ważny od: | Jun 11 10:46:39 2002 GMT |
| Ważny do: | Jun 11 10:46:39 2027 GMT |
| Certyfikat dla Przeglądarek Internetowych | <input type="button" value="Instaluj"/> |
| Certyfikat dla Serwerów WWW i SSL/TLS | <input type="button" value="Instaluj"/> |
| Certyfikat dla urządzeń sieciowych | <input type="button" value="Instaluj"/> |

[do góry ↗](#)

Wyświetlił się interesujący nas certyfikat, który zaznaczymy myszką, wkleimy do pliku i zapiszemy.

UWAGA: W celu wklejania do pliku certyfikatu prezentowanego na stronie należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--", używając do tego celu edytora tekstowego np. Notepad i myszki. **Nie należy używać do tej operacji Worda, czy innego procesora tekstowego!**

W przypadku pobierania certyfikatów pośrednich, wybieramy interesujący nas certyfikat, np. CERTUM Level IV z listy (Certyfikaty Level IV należy pobrać w przypadku, gdy posiadamy certyfikat typu Trusted, certyfikat poziomu III należy pobrać w sytuacji, gdy posiadamy certyfikat typu Enterprise / Wildcard, certyfikat poziomu II należy pobrać w sytuacji, gdy posiadamy certyfikat typu Commercial; dla certyfikatów typu Private pobierany jest certyfikat klasy I). Pozostała część procesu (zapisanie do pliku) przebiega jak dla certyfikatu Certum CA.

1.5. Instalowanie certyfikatu Certum CA i certyfikatów pośrednich

Aby zainstalować główny certyfikat **Certum CA** lub **certyfikaty pośrednie (Certum Level I-IV)** należy z głównego Menu wybrać *Install Trusted Root Certificate into Key Ring*:



W polu *Certificate Label* wpisujemy nazwę certyfikatu. Jeżeli instalujemy certyfikat Certum CA, wpisujemy: *Certum CA*. Po zainstalowaniu tego klucza, powtórzymy całą procedurę dla właściwego certyfikatu pośredniego. W pole *Certificate Label* wpisujemy wtedy np.: *Certum Level IV* lub *Certum Level III*

Wybierz metodę importu certyfikatu – w przypadku opcji *Clipboard* certyfikat należy wkleić w pole *Certificate from Clipboard*; w przypadku wyboru opcji *File*, należy wskazać lokalizację pliku z certyfikatem. Po wypełnieniu powyższych klikamy *Merge Trusted Root Certificate Into Key Ring*.

UWAGA: W celu wklejania certyfikatu należy skopiować fragment tekstu od linii **"--BEGIN CERTIFICATE --"** do **"--END CERTIFICATE--"**, używając do tego celu edytora tekstowego np. Notepad i myszki. **Nie należy używać do tej operacji Worda, czy innego procesora tekstowego!**

Certificate Information

Certificate Label

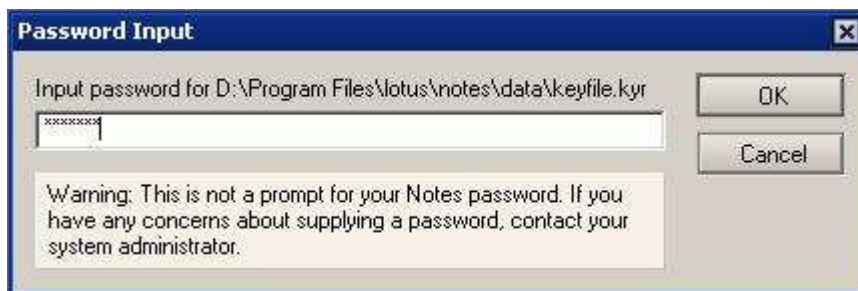
Certificate Source File Clipboard

Certificate from Clipboard:

```

-----BEGIN CERTIFICATE-----
MIIDDDCAfSgAwIBAgIDAQAQMA0GCSqGSIb3DQEBBQUAMD4xCzAJBgNVBAYTA1BM
MRswGQYDVQQKEsJVBm16ZXRvIFNwLiB6IG8ub3R54xEjAQBgNVBAMTCUN1cnRlbSBD
QTAEFw0wMjA2MTEuMDQ2Mz1aFw0yMzA2MTEuMDQ2Mz1aMD4xCzAJBgNVBAYTA1BM
MRswGQYDVQQKEsJVBm16ZXRvIFNwLiB6IG8ub3R54xEjAQBgNVBAMTCUN1cnRlbSBD
QTCASITwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM6xwS7TT3zNjc4Ypk/E
jg+AanPIU1H4m9LcuwBcsaD8dQPugfCI7iNS6eYVM42sLQnFdvkr0YCJ5JdLkKWo
ePhzQ3ukYbDYUMzhhbG2+nPMjX1VjhNWo7/OxLjBos8Q82KxujZlakE403Daaj4GI
ULdtlkIJ89eVgw1BS7Bqa/j8D35in2fE7S2fECPCE/wpFcozo+47UX2bu4lXapu
Ob7kky/ZR6By6/qmW6/KUz/iDsaWWhFu9+lmqSbYf5VT7QqFiLpPKaVCjF62/IUG
AKpoC6EahGcxEZjgoi2IrHu/qpGWX7PNSzVtctpd90gzFFS269lvzs2Ilqsb2pY7
HVkCAwEAAAMTEwDwYDVR0AQH/BAUwAwEB/zANBgkqhkiG9w0BAQUFAA0CAQEAA
uI307+cUus/usESSbLQ5PqKEbq24IXES1HeCh+YgQYHu4vgrt2PRFze+GXKHAQA
T0s9qmdvLdTN/mUxcMUBpgIKumE7bVjCmkn+YzILa+M6wKyr07Do0w1RjBCDxjTg
xSvGzZgFCdsMneNvLJymM/NzD+5yCRCFNZX/OYmQ6kd5YCQzqgNUKD73P9P4Te1q
CjqTE5s7FCMTY5w/OYcneeVMUeMBrYVdGjuxlXMqPnPyvG5k9VpWkKjHDkx0Dy5x
0/fIR/RpbxXyEV6DHpx8Uq79AtoSgFlngMu8cN2bsWntgM6JQEHqDjXKKWYVIZQs
6GAqm4VKQPHriitSbhYscw==
-----END CERTIFICATE-----
    
```

Kreator poprosi o hasło zabezpieczające nasz klucz *keyfile.kyr*:



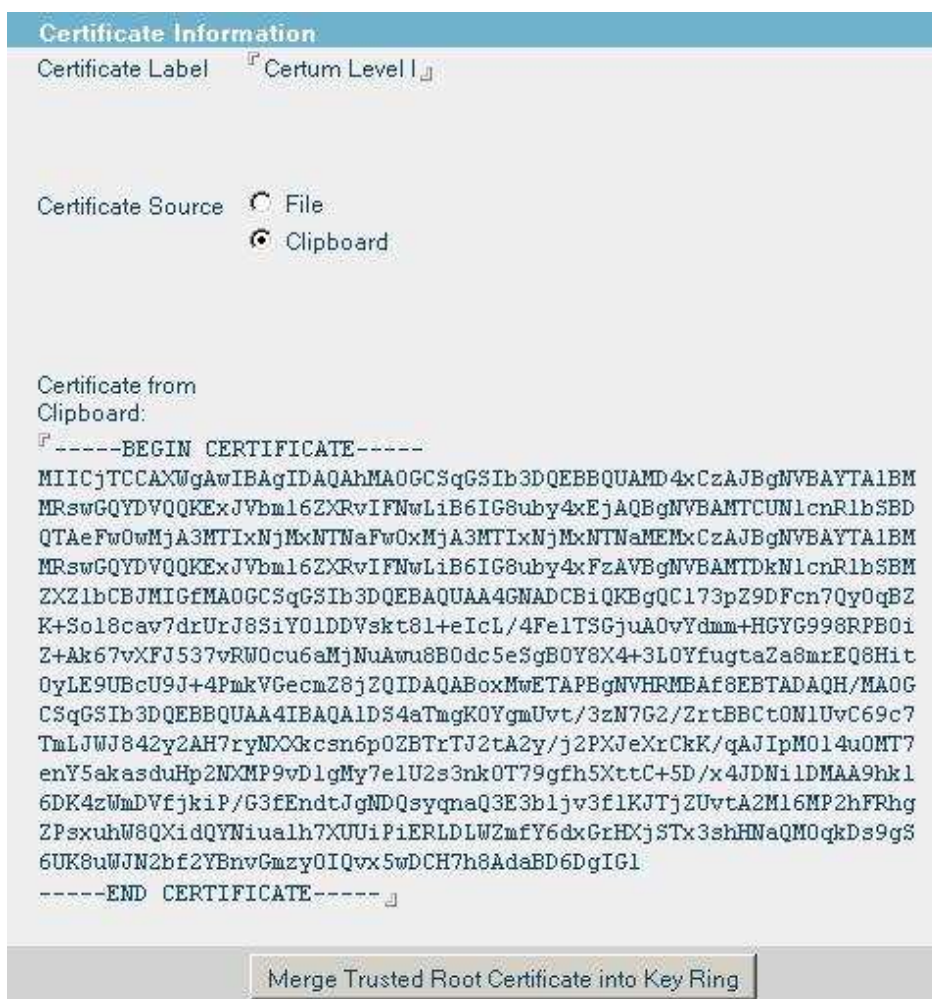
Kreator potwierdza dane certyfikatu:



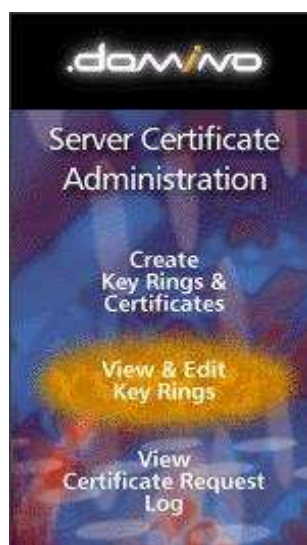
I informuje o pomyślnym zaimportowaniu certyfikatu:



W przypadku importowania certyfikatu pośredniego zmiany dotyczą jedynie innej nazwy certyfikatu (pole *Certificate Label*) oraz innej zawartości samego certyfikatu, wskazywanego z pliku lub wklejanego ze schowka (*Clipboard*):



Po instalacji certyfikatów, możemy sprawdzić ich poprawne dodanie do listy zaufanych urzędów. W tym celu z lewego panelu z głównego *Menu* wybieramy *View & Edit Key Rings*:



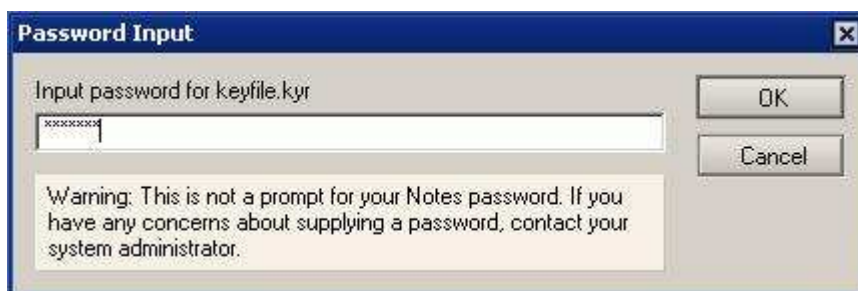
Wybieramy opcję *Select Key Ring to Display*:



Podajemy nazwę pliku *Key Ring*:



I hasło zabezpieczające:



Wyświetlony ekran pozwala sprawdzić poprawność procesu (poniżej: certyfikaty Certum CA i Certum Level I poprawnie dodane do listy zaufanych urzędów certyfikacji).

| Select Key Ring to Display Change Key Ring Password Dump Key Ring To Text Main Menu | | | |
|---|--------------|--|--|
| Certificate Entry Label | Trusted Root | Key Ring | |
| Site Certificates | | | |
| KeyPair | No | D:\Program Files\lotus\notes\data\keyfile. | |
| Certification Authorities | | | |
| Certum Level I | Yes | D:\Program Files\lotus\notes\data\keyfile. | |
| Certum CA | Yes | D:\Program Files\lotus\notes\data\keyfile. | |

1.6. Pobieranie i instalowanie certyfikatu serwera

Aby zainstalować certyfikat na serwerze należy **koniecznie** zakończyć czynności opisane powyżej.

Po wykonaniu powyższych czynności możemy wejść na stronę, której adres otrzymaliśmy pocztą elektroniczną i aktywować certyfikat (umieścić certyfikat w naszym repozytorium dostępnym na stronach www):

ID instalacyjne certyfikatu: b7b1610e652ec1bddbd7e247508dca82a8a5e6a9

Proszę wkleić ID na stronie:
<https://www.certum.pl/install/>

--
Zespół Unizeto CA
info@certum.pl

Wchodzimy na stronę, wklejamy ID i aktywujemy certyfikat klikając *Dalej*:

Instalacja certyfikatu

Wpisz numer certyfikatu który dostałeś w mailu od CERTUM:

Uwaga!

W przypadku certyfikatów e-mail instalacja podpisu powinna odbywać się na tym samym komputerze i przy pomocy tej samej przeglądarki, której używałeś podając adres e-mail.

Pojawi się okno ze szczegółami naszego certyfikatu:


Instalacja certyfikatu

| | |
|---|----------------------|
| Private WEB Server | ważny do: 13.06.2007 |
| Podmiot: 10.100.10.122 | |
| Email: mproszkiewicz@certum.pl | |
| Numer: 0x37CCC | |
| <input type="button" value="Instaluj"/> | |

Kopiujemy numer naszego certyfikatu, wchodzimy na stronę <https://www.certum.pl/services/search.html> i w polu *Nr seryjny*: wpisujemy numer naszego certyfikatu:

Wyszukaj certyfikat (niekwalifikowany)

Wyszukaj certyfikat

 Wpisz adres e-mail lub nazwę podmiotu (imię i nazwisko lub adres serwera www) lub numer seryjny aby odnaleźć certyfikat.

E-mail:
Nazwa podmiotu:
Nr seryjny:

Pojawi się strona, z której będziemy mogli ściągnąć nasz certyfikat w formie binarnej lub tekstowej. Klikamy w *Zapisz tekstowo*:

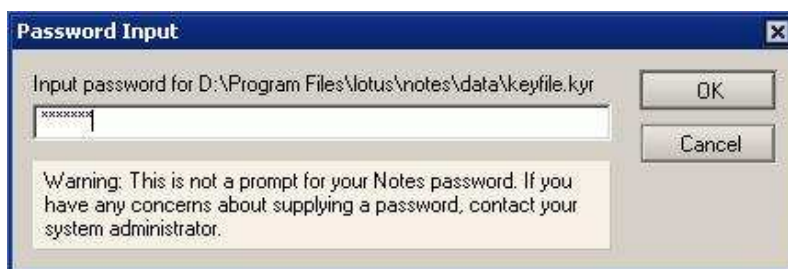
Wyszukaj certyfikat (niekwalifikowany)

| | | |
|--|--|--|
| Private WEB Server | Ważny do: 13-06-2007 | |
| Podmiot: 10.100.10.122 | | |
| Numer: 0x37CCC | | |
| Status: Ważny | | |
| <input type="button" value="Zainstaluj własny"/> | <input type="button" value="Zapisz binarnie"/> | <input type="button" value="Zapisz tekstowo"/> |

Po zapisaniu pliku z certyfikatem należy z głównego menu wybrać opcję *Install Certificate into Key Ring*, wskazać plik klucza *Key Ring* (najlepiej jego dokładną ścieżkę) oraz plik, w którym zapisaliśmy certyfikat naszego serwera.



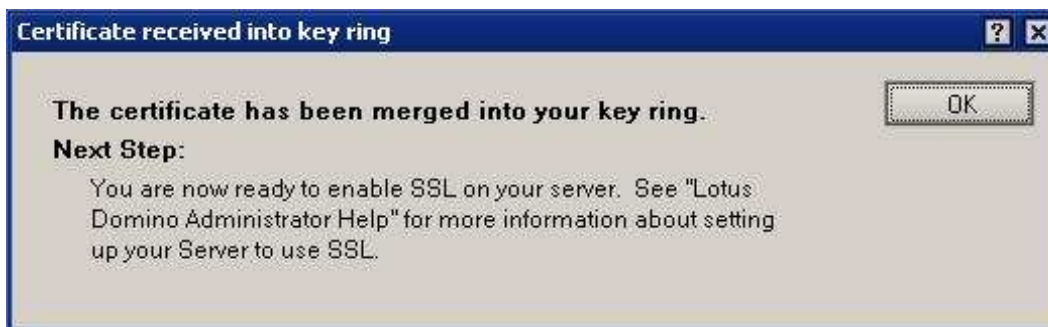
Wpisujemy hasło zabezpieczające plik z kluczem *keyfile.kyr*:



Kreator wyświetli podsumowanie wykonanej operacji.

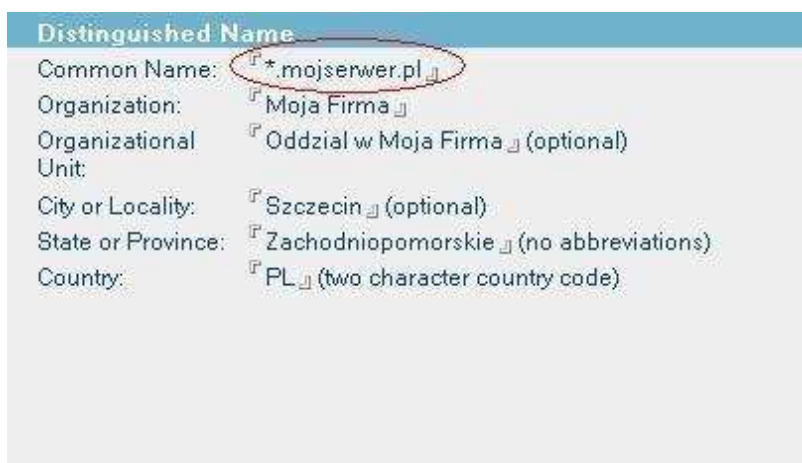


Kreator poinformuje nas o pomyślnym wykonaniu instalacji certyfikatu na serwerze:



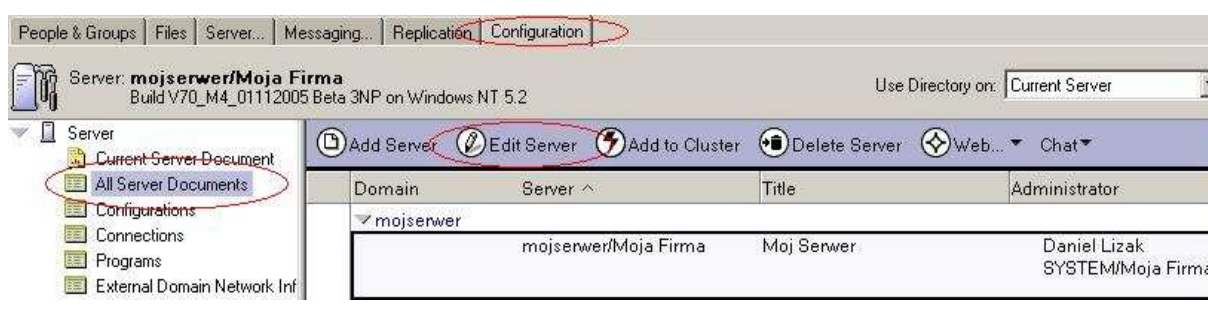
2. Tworzenie certyfikatu dla adresów wieloznacznych

W przypadku tworzenia certyfikatów dla adresów wieloznacznych (np. *.mojafirma.pl), należy wykonać procedurę analogiczną jak opisana powyżej (dla adresów jednoznacznych). Należy jednakże pamiętać, aby przy wypełnianiu danych *Key Ring* wpisać odpowiednią nazwę serwera.



3. Konfigurowanie serwera do połączeń https

W celu skonfigurowania serwera Lotus Domino do połączeń *https* należy w panelu *Configuration* rozwinąć zakładkę *Server* i wejść w *All Server Documents*. Klikamy na dokumentację serwera i edytujemy ją przy pomocy *Edit Server*:

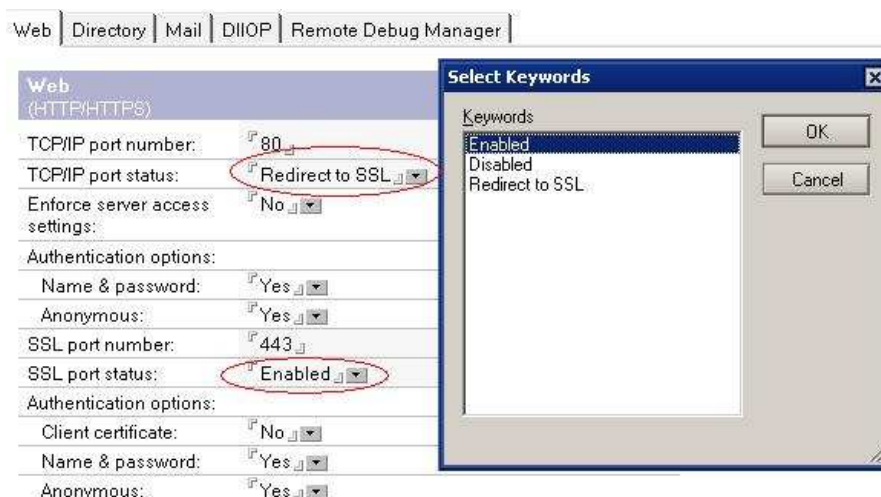


W zakładce *Ports* wybieramy *Internet Ports*:

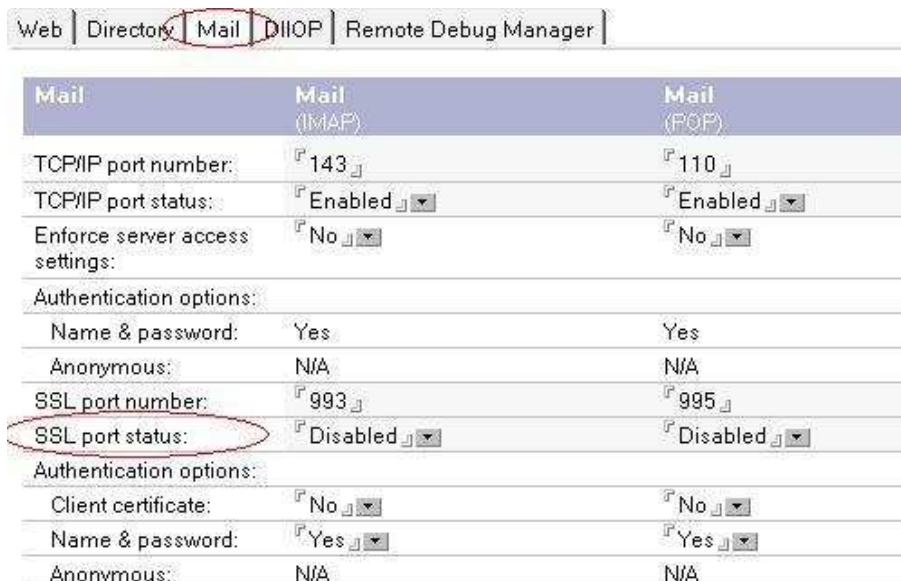


W przypadku serwera WWW, w zakładce *Web* zmieniamy wartości dwóch pól:

- *SSL port status* – zaznaczamy *Enabled*. Spowoduje uruchomienie demona serwera dla połączeń szyfrowanych.
- *TCP/IP port status* – jeżeli chcemy wymusić sesję szyfrowaną zaznaczamy opcję *Redirect to SSL*. Zaznaczenie tej powoduje przełączenie komunikacji na połączenie bezpieczne (*https*), niezależnie od sposobu nawiązania połączenia klienta z serwerem. Opcja *Enabled* powoduje nasłuchiwanie serwera i na porcie dla połączeń zwykłych *http* i szyfrowanych *https*. Z kolei opcja *Disabled* odrzuca wszelkie próby nawiązania połączenia przez połączenie zwykłe.



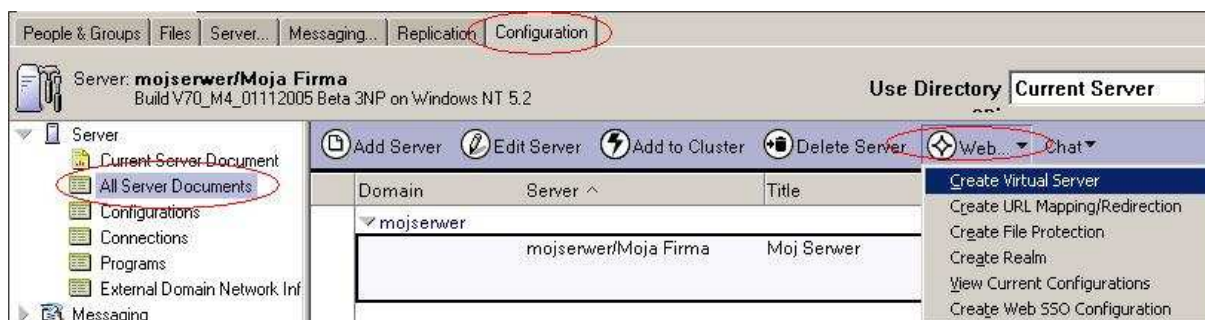
W przypadku serwera pocztowego, zmian dokonujemy w zakładce *Mail*. W zależności od konfiguracji serwera pocztowego, połączenia SSL możemy aktywować dla konkretnych protokołów. W tym celu pole *SSL port status* danego protokołu należy zmienić *Disabled* na *Enabled*. W tym momencie demon pocztowy nasłuchiwał będzie zarówno na porcie szyfrowanym jak i nieszyfrowanym. Aby “wymusić” sesje tylko i wyłącznie tunelowane, należy zmienić wartość pola *TCP/IP port status*, na *Redirect to SSL*.



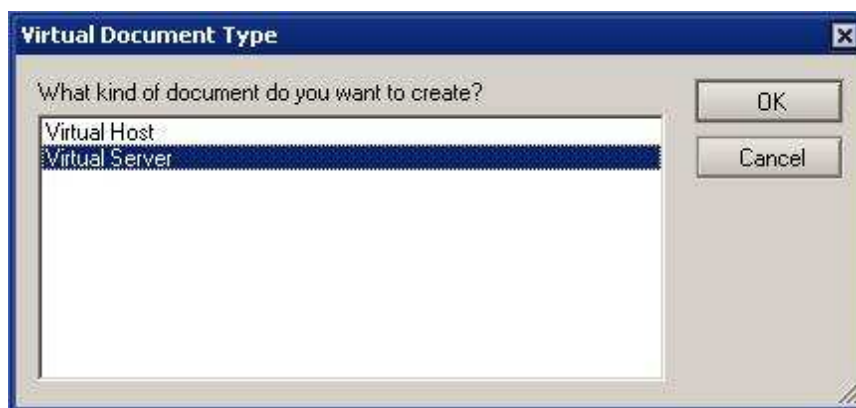
W obu przypadkach, w celu zapamiętania zmian restartujemy serwer z poziomu konsoli: *restart server haslo_do_servera*

4. Konfigurowanie serwera do obsługi witryn wirtualnych

W celu skonfigurowania serwera Lotus Domino do obsługi wielu witryn wirtualnych w otoczeniu SSL należy w panelu *Configuration* rozwinąć zakładkę *Server* i wybrać opcję *All Server Documents*. Ze środkowego *Menu* rozwijamy zakładkę *Web...* i chodzimy w *Create Virtual Server*.



Do wyboru są dwie opcje. Jeżeli wirtualny serwer znajduje się na lokalnej maszynie należy wybrać *Virtual Host*. W przypadku, gdy wirtualna witryna znajduje się poza lokalnym hostem – należy wybrać *Virtual Server*.



Wpisujemy adres IP hosta, na którym znajduje się wirtualna witryna (w przypadku gdy jest to lokalny host wpisujemy 127.0.0.1). W polu *Hostname* wprowadzimy **DNS** naszego serwera:



The screenshot shows the 'VIRTUAL SERVER for mojserwer/Moja Firma' configuration window. The 'Site Information' tab is active. The fields are: IP address: 192.168.129.209, Hostname: (Optional) poddomena1.mojserwer.pl, Comments: , and Default home page: default.htm. The IP address and Hostname fields are circled in red.

Przełączamy się na sąsiednią zakładkę *Mapping*. Wpisujemy nazwę pliku, który domyślnie będzie wyświetlany po połączeniu z serwerem. Wskazujemy katalog, w którym znajduje się ten plik.



The screenshot shows the 'VIRTUAL SERVER for mojserwer/Moja Firma' configuration window. The 'Mapping' tab is active. The fields are: Home URL: index.html, HTML directory: domino\moj_katalog, Icon directory: dominol\icons, Icon URL path: /icons, CGI directory: domino\cgi-bin, and CGI URL path: /cgi-bin. The Home URL and HTML directory fields are circled in red.

Czynności powyższe powtarzamy dla każdej poddomeny: poddomena1, poddomena2 itp. Nie zapomnij zapisać zmian *Save&Close* oraz zrestartować serwer z poziomu konsoli poleceniem: *tell http restart*.