

Routerzy QNO

Instalacja certyfikatów SSL w routerach

QVF74xx



Poznań 2011

1. Cel instrukcji

Instrukcja opisuje generowanie i instalację na routerze oraz komputerach klientów certyfikatów SSL, wykorzystywanych przy zarządzaniu urządzeniem za pomocą protokołu https oraz przy zestawianiu połączeń VPN SSL.

2. Założenia

Routery QNO serii QVF74xx oferują możliwość zarządzania urządzeniem za pomocą szyfrowanego protokołu https oraz tworzenia tuneli VPN typu Client to Gateway z wykorzystaniem technologii SSL. Domyślnie routery QNO posiadają zainstalowany certyfikat SSL, wygenerowany dla domeny qno.com.tw (czyli strony głównej producenta routerów). W związku z tym, że każdy router docelowo będzie znajdował się pod określoną przez jego administratora nazwą domenową lub adresem IP, aby uniknąć problemów związanych z błędami występującymi w domyślnym certyfikacie SSL (wynikającymi z niezgodności nazwy w certyfikacie z adresem pod którym jest router), należy po zainstalowaniu routera wygenerować unikalny dla niego certyfikat.

W routerach dostępne są 2 metody instalacji certyfikatów SSL:

- import do routera certyfikatu wydanego przez CA (Certificate Authority), czyli autoryzowanego dostawcę certyfikatów
- wygenerowanie na routerze własnego certyfikatu (jako CA występuje wtedy sam router) i przeniesienie certyfikatu na komputery które z routerem będą się łączyły.

Obie metody mają swoje wady i zalety, w przypadku pierwszym proces generowania certyfikatu jest bardziej złożony, ponieważ w pierwszym kroku należy wygenerować na routerze plik CSR (Certificate Signing Request) a następnie dostarczyć plik do autoryzowanego wystawcy certyfikatów, gdzie na jego podstawie wygenerowany zostanie certyfikat dla routera i następnie wgrać ten certyfikat na router. Najczęściej wiąże się to z dodatkowymi kosztami jakie musi ponieść klient, w związku z wystawieniem certyfikatu przez CA. Zaletą tej metody jest jednak fakt, że certyfikatu w większości wypadków nie będzie trzeba przynosić na komputery klienckie ponieważ, przeglądarki posiadają wbudowaną listę autoryzowanych CA których certyfikatom ufają z założenia.

W przypadku drugim, to router sam stanowi CA, czyli nie trzeba generować pliku CSR i wysłać go do autoryzowanego dostawcy oraz ponosić dodatkowych kosztów związanych z generowaniem certyfikatu. Minusem tego rozwiązania jest fakt, że certyfikat musi zostać zainstalowany na komputerach klienckich które będą podłączać się do routera.

Ponieważ, sam proces importu certyfikatu do routera jest analogiczny w obu wypadkach, w dalszej części opisano metodę generowania własnego certyfikatu na routerze oraz jego późniejszej instalacji na komputerze klienckim.

3. Generowanie i instalacja certyfikatu na routerze

Po zainstalowaniu routera w miejscu docelowym (nadaniu docelowej adresacji IP, lub przypisaniu nazwy domenowej) należy w pierwszym kroku wygenerować unikalny dla niego certyfikat SSL. Podstawowe wskazówki do konfiguracji wstępnej routerów QNO można znaleźć w instrukcji:

ftp://ftp.fen.pl/instrukcje/QNO/QNO_podstawowa_konfiguracja.pdf

Aby wygenerować certyfikat dla routera należy po zalogowaniu się na jego interfejs administracyjny przejść do zakładki (na tym etapie przy logowaniu do routera będziemy obserwować jeszcze błędy związane z nieprawidłowym certyfikatem): Advanced SSL VPN -> Certificate Management

The screenshot shows the QNO router's web interface. The sidebar on the left contains navigation links: Home, Network, Internet Filter, USB Setting, QoS, IP/DHCP, Group Management, Firewall, Advanced Function, System Tool, Port Management, and VPN. Under the VPN section, 'Advanced SSL VPN' is selected, with sub-links for Status, Group Summary, Group Management, Domain Management, User Management, Resource Management, Link to portal, Certificate Management (highlighted), and Advanced Settings.

The main content area displays the 'Server Certificate Table' and 'List of trusted CA certificate'.

Server Certificate Table

In Use	Subject	Issuer	Expiration Date	View Detail	Delete
<input checked="" type="radio"/>	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/email Address=fae@qno.com.tw	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/email Address=fae@qno.com.tw	Jul 9 02:13:16 2012 GMT		

List of trusted CA certificate

Trust	Subject	Issuer	Expiration Date	View Detail	Delete
<input checked="" type="checkbox"/>	/O=Entrust.net/OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liability)/OU=(c) 1999 Entrust.net Limited/CN=Entrust.net Certification Authority (2048)	/O=Entrust.net/OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liability)/OU=(c) 1999 Entrust.net Limited/CN=Entrust.net Certification Authority (2048)	Dec 24 18:20:51 2019 GMT		
<input checked="" type="checkbox"/>	/C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root	/C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT		
<input checked="" type="checkbox"/>	/C=US/O=Equifax Secure Inc./CN=Equifax Secure Global eBusiness CA-1	/C=US/O=Equifax Secure Inc./CN=Equifax Secure Global eBusiness CA-1	Jun 21 04:00:00 2020 GMT		
<input checked="" type="checkbox"/>	/C=US/O=Equifax Secure Inc./CN=Equifax Secure eBusiness CA-1	/C=US/O=Equifax Secure Inc./CN=Equifax Secure eBusiness CA-1	Jun 21 04:00:00 2020 GMT		
<input checked="" type="checkbox"/>	/C=US/O=Equifax Secure/OU=Equifax Secure eBusiness CA-2	/C=US/O=Equifax Secure/OU=Equifax Secure eBusiness CA-2	Jun 23 12:14:45 2019 GMT		
<input checked="" type="checkbox"/>	/C=US/O=VISA/OU=Visa International Service Association/CN=GP Root 2	/C=US/O=VISA/OU=Visa International Service Association/CN=GP Root 2	Aug 15 23:59:00 2020 GMT		
<input checked="" type="checkbox"/>	/C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Class 1 CA Root	/C=SE/O=AddTrust AB/OU=AddTrust TTP Network/CN=AddTrust Class 1 CA Root	May 30 10:38:31 2020 GMT		
<input checked="" type="checkbox"/>	/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting/OU=Certification Services Division/CN=Thawte Personal Basic CA/emailAddress=cert@thawte.com	/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting/OU=Certification Services Division/CN=Thawte Personal Basic CA/emailAddress=cert@thawte.com	Dec 31 23:59:59 2020 GMT		

W dolnej części strony dostępne są dwie opcje generowania certyfikatów:

- Generate CSR for third-party certificate request – generowanie pliku CSR dla autoryzowanego wystawcy certyfikatów CA.
- Generate self-signed certificate – wygenerowanie certyfikatu dla routera bezpośrednio na nim

▶ Server Certificate Generation

Subject	
Country Name:	<input type="text"/>
Province Name:	<input type="text"/>
Locality Name:	<input type="text"/>
Organization:	<input type="text"/>
Department:	<input type="text"/>
Common Name:	<input type="text"/> * required
E-mail	<input type="text"/>
Key Encryption Length:	<input type="text" value="512"/> * required
Valid Duration:	<input type="text"/> * required(unit days) (e.g.365)

Zgodnie z przyjętymi założeniami, po wypełnieniu pól takich jak:

Country Name – Kod kraju – dwucyfrowy kod kraju w którym pracuje urządzenie np. **PL**

Province Name – Określenie regionu/województwa – np. **Wielkopolskie**

Locality Name – Bardziej szczegółowe określenie lokalizacji/miasto – np. **Poznan**

Organization – Organizacja która wykorzystuje certyfikat – np. **Konsorcjum FEN**

Department – Dział organizacji do którego przypisany jest certyfikat – np. **Support**

Common Name – publiczny adres routera, nazwa domenowa lub adres IP – np. **80.53.97.174**

E-mail – adres email – np. support@fen.pl

Key Encryption Length – długość klucza szyfrowania – np. **512**

Valid Duration – czas do wygaśnięcia certyfikatu wyrażony w dniach – np. **365**

Po wypełnieniu pól zgodnie z przedstawionym wzorcem np.

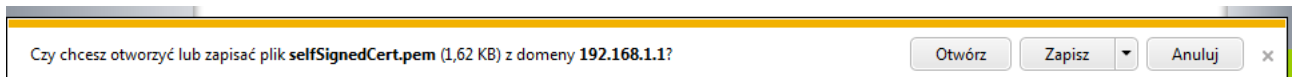
Server Certificate Generation

Subject	
Country Name:	PL
Province Name:	Wielkopolskie
Locality Name:	Poznan
Organization:	Konsorcjum FEN
Department:	Support
Common Name:	80.53.97.174 * required
E-mail:	support@fen.pl
Key Encryption Length:	512 * required
Valid Duration:	365 * required(unit:days) (e.g.365)

Generate CSR for third-party certificate request Generate self-signed certificate

Należy wybrać opcję Generate self-signed certificate.

Po jej wybraniu router powinien wyświetlić monit o pobranie pliku selfSignedCert.pem

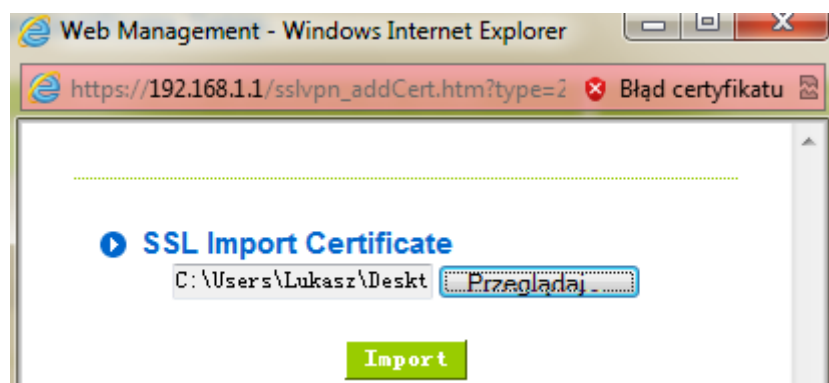


Po zapisaniu pliku na komputerze klienckim należy przejść do górnej części strony i wybrać opcję Add:

Server Certificate Table

In Use	Subject	Issuer	Expiration Date	View Detail	Delete
<input checked="" type="radio"/>	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/email Address=fae@qno.com.tw	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/email Address=fae@qno.com.tw	Jul 9 02:13:16 2012 GMT		

Następnie należy wskazać plik który przed chwilą został zapisany na komputerze w formie selfSignedCert.pem





Po wybraniu opcji Import nowy certyfikat powinien pojawić się na routerze:

Server Certificate Table

Add		Export Used Certificate for Client	Export Used Certificate for Administrator		
In Use	Subject	Issuer	Expiration Date	View Detail	Delete
<input checked="" type="radio"/>	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/emailAddress=fae@qno.com.tw	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/emailAddress=fae@qno.com.tw	Jul 9 02:13:16 2012 GMT		
<input type="radio"/>	/C=PL/ST=Wielkopolskie/L=Poznan/O=Konsorcjum 0.000000EN/OU=Support/CN=80.53.97.174/emailAddress=support@fen.pl	/C=PL/ST=Wielkopolskie/L=Poznan/O=Konsorcjum-5314010372517808256365875999042120126393966197323471728421288900973994994995621064806304670425032319319930465788549226676808739915925371739460987196007348791827079941548676023768610333732891248836776279058553813468132083187809672236108475372289683798186194185572396939187224601663273871174881037181255680.000000EN/OU=Support/CN=80.53.97.174/emailAddress=support@fen.pl	Nov 14 08:39:15 2012 GMT		

Aby router zaczął korzystać z nowego certyfikatu należy zaznaczyć nowy certyfikat:

Server Certificate Table

Add		Export Used Certificate for Client	Export Used Certificate for Administrator		
In Use	Subject	Issuer	Expiration Date	View Detail	Delete
<input type="radio"/>	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/emailAddress=fae@qno.com.tw	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/emailAddress=fae@qno.com.tw	Jul 9 02:13:16 2012 GMT		
<input checked="" type="radio"/>	/C=PL/ST=Wielkopolskie/L=Poznan/O=Konsorcjum 0.000000EN/OU=Support/CN=80.53.97.174/emailAddress=support@fen.pl	/C=PL/ST=Wielkopolskie/L=Poznan/O=Konsorcjum-5314010372517808256365875999042120126393966197323471728421288900973994994995621064806304670425032319319930465788549226676808739915925371739460987196007348791827079941548676023768610333732891248836776279058553813468132083187809672236108475372289683798186194185572396939187224601663273871174881037181255680.000000EN/OU=Support/CN=80.53.97.174/emailAddress=support@fen.pl	Nov 14 08:39:15 2012 GMT		

i wybrać opcję Apply, znajdującą się pod listą wszystkich zaufanych certyfikatów które router ma zainstalowane(przycisk znajduje się u dołu strony):



Po tej operacji nowy certyfikat stanie się aktywnym na routerze, co można stwierdzić sprawdzając przy którym certyfikacie znajduje się zaznaczenie(niebieskie kółko) oraz brakiem ikony kosza przy aktywnym certyfikacie.

4. Instalacja certyfikatu na komputerach klientów

Po zainstalowaniu certyfikatu na routerze należy certyfikat ten zainstalować również na komputerach klientów.

Można to przeprowadzić na 2 sposoby:

- pobierając certyfikat dla klienta za pomocą paska przeglądarki IE przy ponownym zalogowaniu się na router
- pobierając certyfikat dla klienta, bezpośrednio z routera(Export Certificate for Client) i instalując go przez konsolę systemu Windows - msc

4.1 Instalacja certyfikatu z wykorzystaniem paska przeglądarki IE

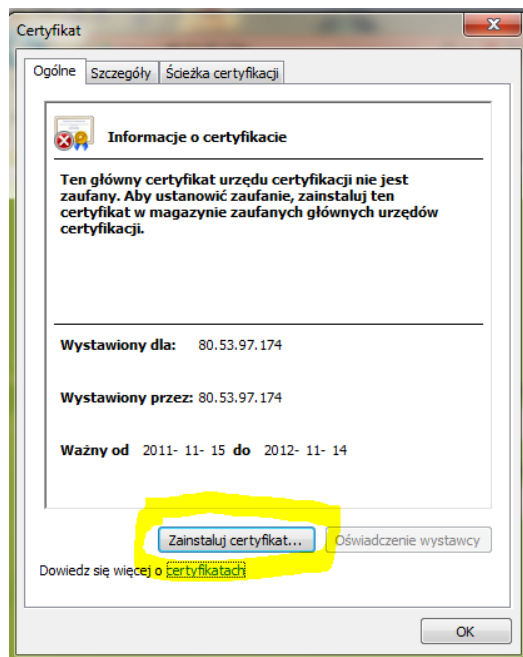
Po wylogowaniu się z routera, należy zamknąć aktywne okno przeglądarki i zalogować się na router z nowego okna.

Przeglądarka nadal będzie w tym momencie wyświetlać błędy certyfikatów:

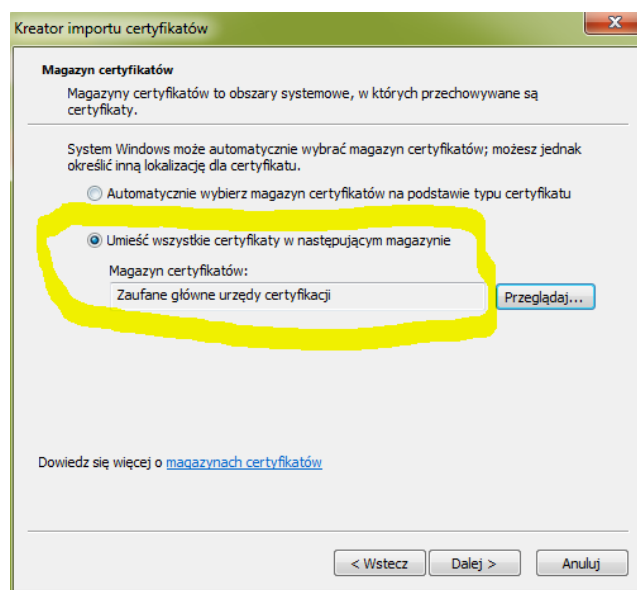


Należy kliknąć lewym przyciskiem myszy na wyświetlający się błąd i wybrać opcję wyświetl certyfikaty.

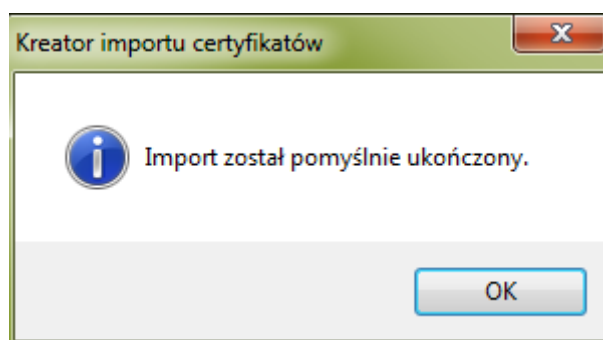
Po jej wybraniu pojawi się nowy certyfikat wystawiony dla adresu naszego routera który można zainstalować wybierając przycisk Zainstaluj Certyfikat.



Po jego wybraniu pojawi się kreator Importu certyfikatów, w drugim kroku pracy kreatora należy wybrać opcję: Umieść wszystkie certyfikaty w następującym magazynie: Zaufane główne urzędy certyfikacji.

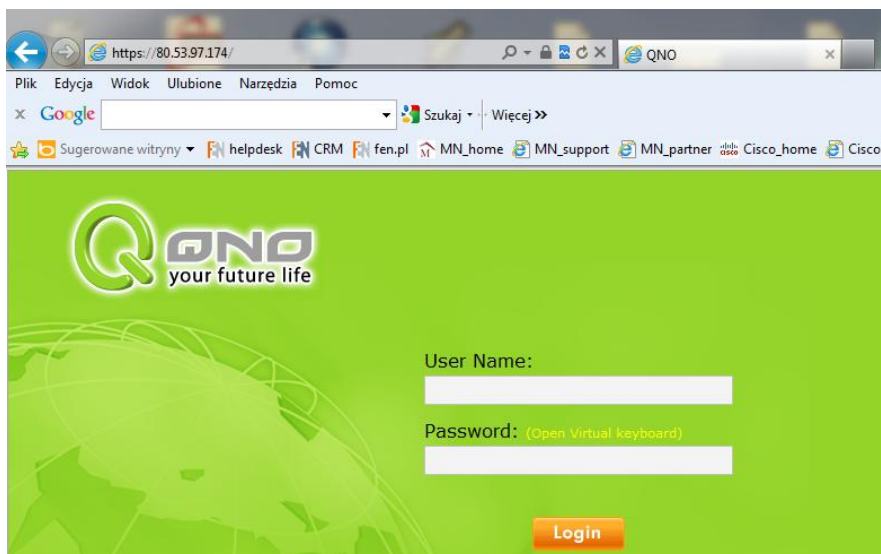


Kontynuując pracę kreatora poprzez wybranie opcji dalej i zatwierdzenie w kolejnych krokach poprawności certyfikatu który chcemy zainstalować powinniśmy zakończyć prace kreatora na informacji:



Aby potwierdzić, czy certyfikat został zainstalowany na komputerze poprawnie, należy zamknąć przeglądarkę i uruchomić ją ponownie.

Wpisując tym razem w pasek adresu, zewnętrzny adres pod jakim dostępny jest router błąd związany z certyfikatem nie powinien się pojawić:



Poprawność certyfikatu możemy stwierdzić wyświetlając go poprzez skorzystanie z przyciska kłódki znajdującego się w pasku adresowym.

4.2 Instalacja certyfikatu za pośrednictwem konsoli msc systemu Windows

W przypadku problemów z instalacją certyfikatu za pośrednictwem przeglądarki IE certyfikat należy zainstalować za pomocą konsoli msc systemu Windows.

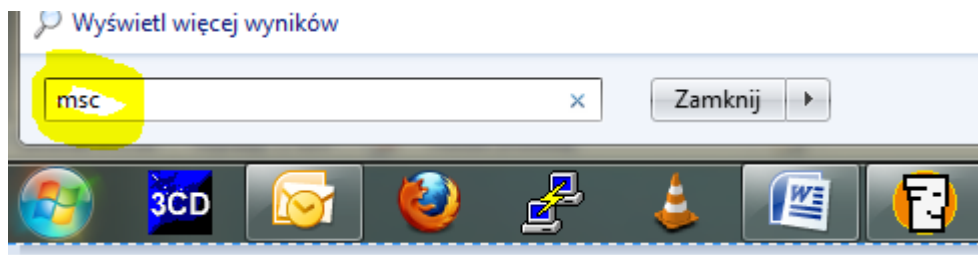
W pierwszym kroku należy pobrać certyfikat dla klienta z routera, można to zrobić korzystając z opcji:

Export Used Certificate for Client

Server Certificate Table						
Add	Export Used Certificate for Client		Export Used Certificate for Administrator			
In Use	Subject	Issuer	Chain Certificate	Expiration Date	View Detail	Delete
<input type="radio"/>	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw/emailAddress=fae@qno.com.tw	/C=TW/ST=Hsinchu/L=Hsinchu/O=Qno Technology Inc./OU=Product Development/CN=qno.com.tw		Jul 9 02:13:16 2012 GMT		
<input checked="" type="radio"/>	/C=PL/ST=Wielkopolskie/L=Poznan/O=FEN/OU=Support/CN=192.168.100.104/emailAddress=support@fen.pl	/C=PL/ST=Wielkopolskie/L=Poznan/O=FEN/OU=Support/CN=192.168.100.104/emailAddress=support@fen.pl	Disabled	Nov 14 11:18:22 2012 GMT		

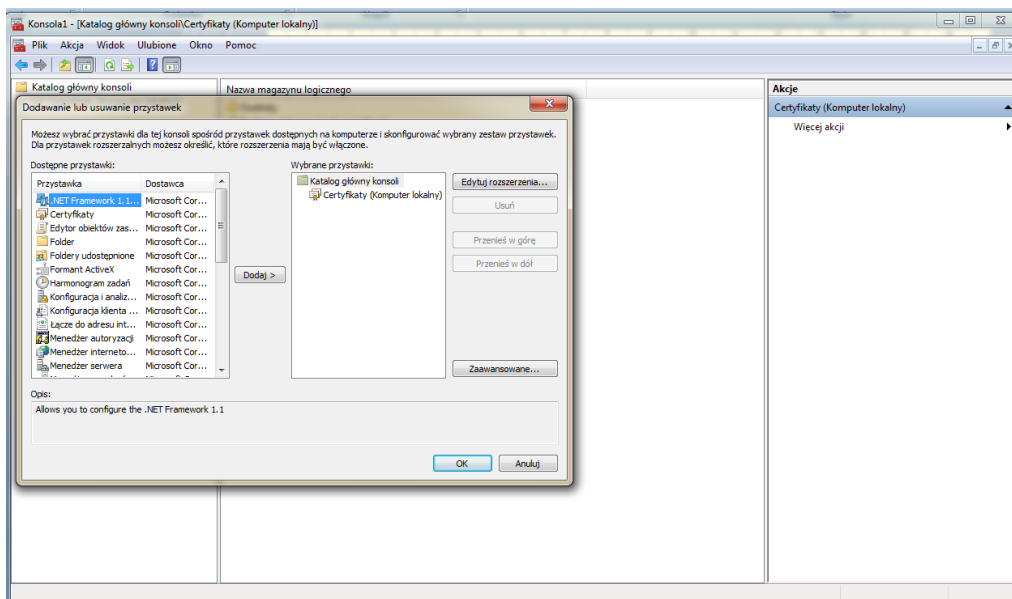
Po jej wybraniu na komputerze zapisany zostanie plik w postaci: SSL005v2_1114_1609.pem , który będzie potrzebny w kolejnych krokach instalacji certyfikatu przez konsolę msc.

Aby uruchomić konsolę msc należy po przejściu do zakładki Uruchom w Menu Start wpisać: msc i zatwierdzić przyciskiem Enter.



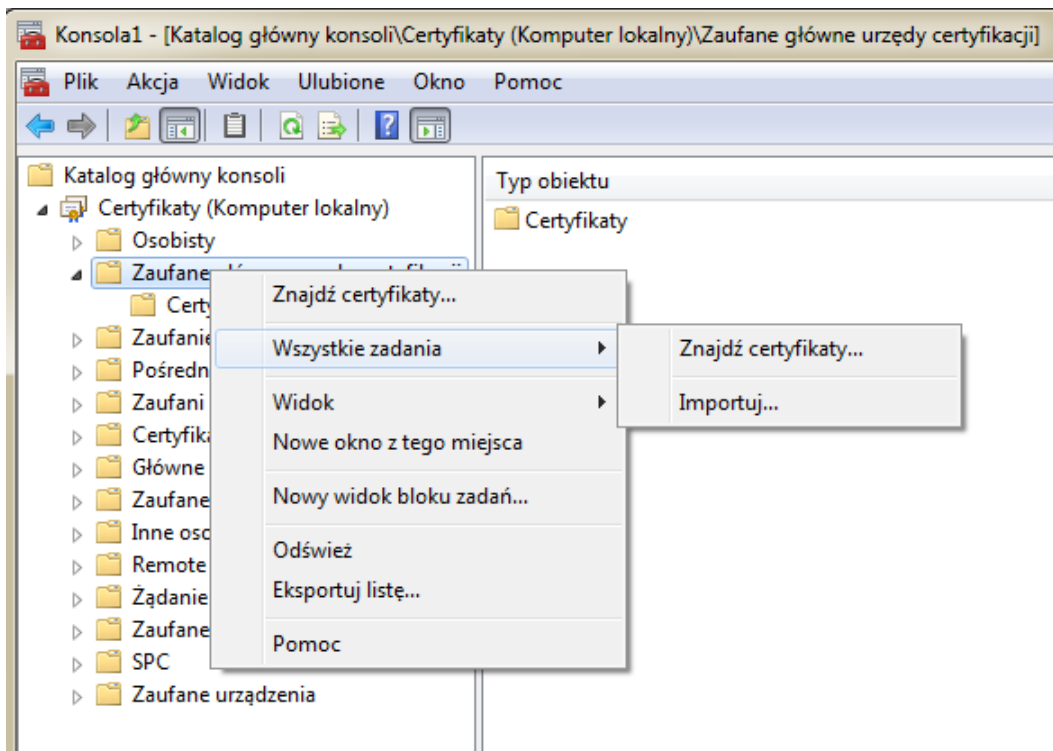
Po wprowadzeniu komendy powinna uruchomić się konsola msc.

Korzystając z menu Plik należy wybrać opcję Dodaj lub Usuń przystawkę.

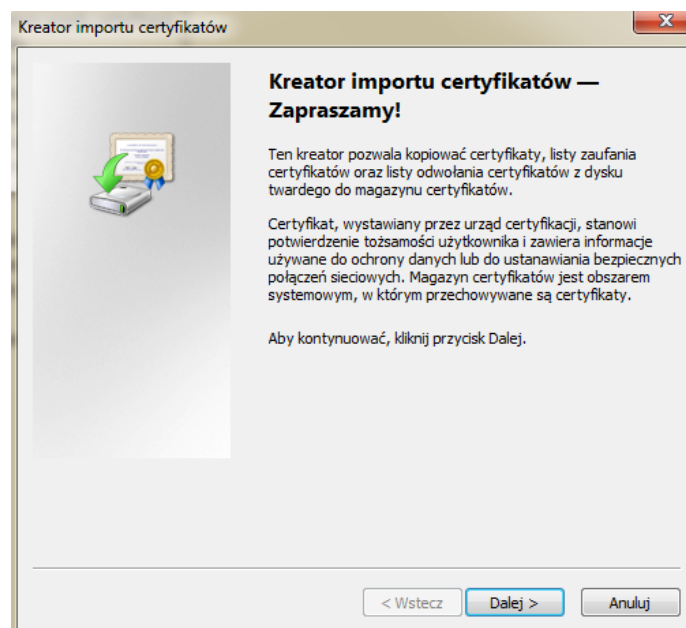


Z dostępnych przystawek należy wybrać opcję Certyfikaty, kliknąć przycisk Dodaj i zatwierdzić klawiszem OK.

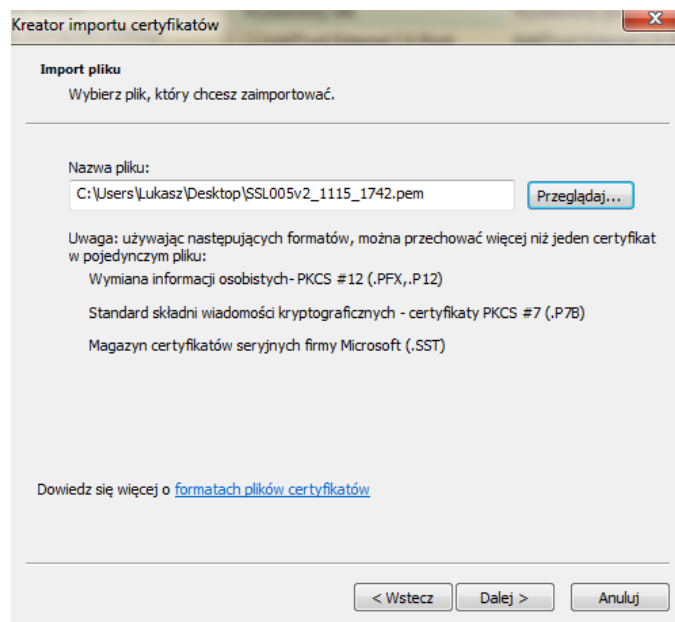
W pasku konsoli w przystawce Certyfikaty należy, rozwinąć drzewo, tak aby wyświetlić, Zaufane główne urzędy certyfikacji, kliknąć na nie prawym przyciskiem myszy i z menu: „Wszystkie zadania” wybrać opcję „Importuj”.



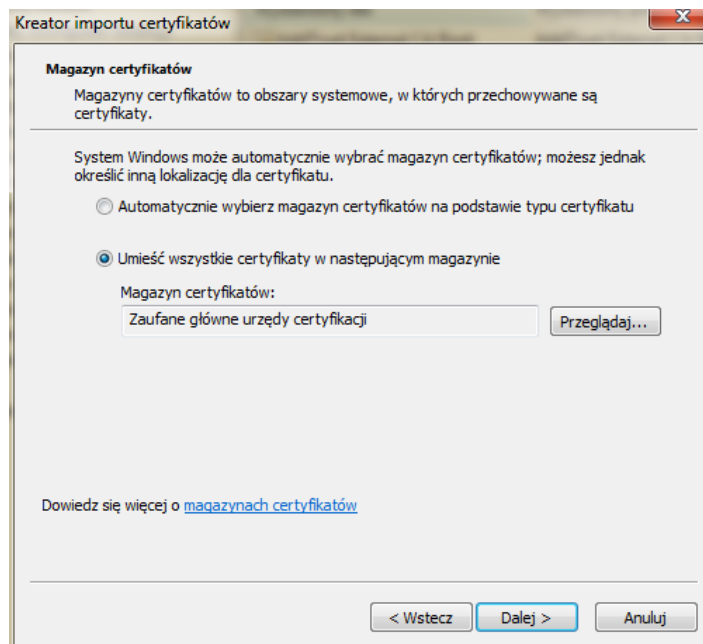
Uruchomi się kreator Importu certyfikatów.



W drugim oknie kreatora należy wskazać plik certyfikatu przeniesiony z routera w postaci: SSL005v2_1114_1609.pem



Wskaż lokalizację dla certyfikatu jako zaufane główne urzędy certyfikacji.



Działanie kreatora powinno zakończyć się informacją Import pomyślnie ukończony.

Przy kolejnym uruchomieniu przeglądarki błąd związany z certyfikatami nie powinien się już pojawić.

Gwarancja:

Konsorcjum FEN Sp. z o.o. prowadzi serwis gwarancyjny produktów oferowanych w serwisie dealerskim www.fen.pl.

Procedury dotyczące przyjmowania urządzeń do serwisu są odwrotne do kanału sprzedaży tzn.: w przypadku uszkodzenia urządzenia przez klienta końcowego, musi on dostarczyć produkt do miejsca jego zakupu.

Skrócone zasady reklamacji sprzętu:

Reklamowany sprzęt powinien być dostarczony w stanie kompletnym, w oryginalnym opakowaniu zabezpieczającym lub w opakowaniu zastępczym zapewniającym bezpieczne warunki transportu i przechowywania analogicznie do warunków zapewnianych przez opakowanie fabryczne.

Szczegółowe informacje dotyczące serwisu można znaleźć pod adresem www.fen.pl/serwis

Konsorcjum FEN współpracuje z Europejską Platformą Recyklingu ERP w sprawie zbiórki zużytego sprzętu elektrycznego i elektronicznego. Lista punktów, w których można zostawiać niepotrzebne produkty znajduje się pod adresem www.fen.pl/download/ListaZSEIE.pdf

Informacja o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu ("przekreślony śmietnik") nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w wyznaczonych punktach odbioru. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu prosimy się zwrócić do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Powyższa instrukcja jest własnością Konsorcjum FEN Sp. z o.o.



Dział Wsparcia Technicznego

Konsorcjum FEN Sp. z o.o.

Kontakt: help@fen.pl
